Códigos electrónicos

Código del Derecho al Olvido

Selección y ordenación:
Luis Gervas de la Pisa
VIDAU ABOGADOS

Edición actualizada a 14 de julio de 2021

BOLETÍN OFICIAL DEL ESTADO

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/biblioteca_juridica/

Alertas de actualización en Mi BOE: www.boe.es/mi_boe/

Para adquirir el Código en formato papel: tienda.boe.es

© Agencia Estatal Boletín Oficial del Estado
NIPO (PDF): 007-14-193-1
NIPO (Papel): 007-14-192-6
NIPO (ePUB): 007-14-194-7
ISBN: 978-84-340-2158-7
Depósito Legal: M-33795-2014

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
www.boe.es

SUMARIO

§ 1. Nota del autor 1

CONSTITUCIÓN ESPAÑOLA

§ 2. Constitución Española. [Inclusión parcial] 3

NORMATIVA DE PROTECCIÓN DE DATOS

§ 3. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales 14

§ 4. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal 75

§ 5. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) 128

§ 6. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras 218

§ 7. Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo . . 223

§ 8. Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios 225

§ 9. Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal . . 227

§ 10. Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos 229

§ 11. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos 242

SOCIEDAD DE LA INFORMACIÓN

§ 12. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico 255

§ 13. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información 289

NORMATIVA CONEXA

CIVIL

§ 14. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen 321

§ 15. Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación 327

§ 16. Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. [Inclusión parcial] 330

§ 17. Ley 20/2011, de 21 de julio, del Registro Civil 332

§ 18. Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención relativa al sexo de las personas 375

PENAL

§ 19. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial] 379

ADMINISTRACIÓN DE JUSTICIA

§ 20. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial] 388

§ 21. Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional 392

§ 22. Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia 420

§ 23. Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia 450

ADMINISTRACIONES PÚBLICAS

§ 24. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial] 465

§ 25. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. [Inclusión parcial] 471

§ 26. Ley 9/1968, de 5 de abril, sobre secretos oficiales 517

§ 27. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica 521

§ 28. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica 540

MENORES

§ 29. Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil 588

SANITARIA

§ 30. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica 631

BOLETINES OFICIALES

§ 31. Ley 5/2002, de 4 de abril, reguladora de los Boletines Oficiales de las Provincias 643

§ 32. Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado» 650

INDULTOS

§ 33. Ley de 18 de junio de 1870 estableciendo reglas para el ejercicio de la gracia de indulto 669

FUERZAS Y CUERPOS DE SEGURIDAD

§ 34. Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. [Inclusión parcial] 674

§ 35. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN 676

§ 36. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos 682

§ 37. Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. [Inclusión parcial] 689

§ 38. Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas. [Inclusión parcial] 692

§ 39. Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior 717

NORMATIVA PENITENCIARIA

§ 40. Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario. [Inclusión parcial] 923

TELECOMUNICACIONES

§ 41. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones 926

§ 42. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial] 937

§ 43. Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas 941

CONSUMIDORES Y USUARIOS

§ 44. Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. [Inclusión parcial] 961

§ 45. Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios 964

NORMATIVA TRIBUTARIA

§ 46. Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial] 1028

§ 47. Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos. [Inclusión parcial] 1036

SEGURIDAD SOCIAL

§ 48. Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social. [Inclusión parcial] 1042

PUBLICACIÓN DE SANCIONES DE TRÁFICO

§ 49. Orden INT/3022/2010, de 23 de noviembre, por la que se regula el Tablón Edictal de Sanciones de Tráfico 1052

ÍNDICE SISTEMÁTICO

§ 1. Nota del autor 1

CONSTITUCIÓN ESPAÑOLA

§ 2. Constitución Española. [Inclusión parcial] 3

[. . .]

TÍTULO I. De los derechos y deberes fundamentales 3
CAPÍTULO PRIMERO. De los españoles y los extranjeros 3
CAPÍTULO SEGUNDO. Derechos y libertades 4
Sección 1.ª De los derechos fundamentales y de las libertades públicas 4
Sección 2.ª De los derechos y deberes de los ciudadanos 7
CAPÍTULO TERCERO. De los principios rectores de la política social y económica 8
CAPÍTULO CUARTO. De las garantías de las libertades y derechos fundamentales 10
CAPÍTULO QUINTO. De la suspensión de los derechos y libertades 11
TÍTULO II. De la Corona 11

[. . .]

NORMATIVA DE PROTECCIÓN DE DATOS

§ 3. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales 14

Preámbulo 14
TÍTULO I. Disposiciones generales 21
TÍTULO II. Principios de protección de datos 22
TÍTULO III. Derechos de las personas 24
CAPÍTULO I. Transparencia e información 24
CAPÍTULO II. Ejercicio de los derechos 25
TÍTULO IV. Disposiciones aplicables a tratamientos concretos 26
TÍTULO V. Responsable y encargado del tratamiento 31
CAPÍTULO I. Disposiciones generales. Medidas de responsabilidad activa 31
CAPÍTULO II. Encargado del tratamiento 33
CAPÍTULO III. Delegado de protección de datos 33
CAPÍTULO IV. Códigos de conducta y certificación 35
TÍTULO VI. Transferencias internacionales de datos 37
TÍTULO VII. Autoridades de protección de datos 38
CAPÍTULO I. La Agencia Española de Protección de Datos 38
Sección 1.ª Disposiciones generales 38
Sección 2.ª Potestades de investigación y planes de auditoría preventiva 41
Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos 43
CAPÍTULO II. Autoridades autonómicas de protección de datos 44
Sección 1.ª Disposiciones generales 44
Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679 . 45
TÍTULO VIII. Procedimientos en caso de posible vulneración de la normativa de protección de datos 46
TÍTULO IX. Régimen sancionador 49
TÍTULO X. Garantía de los derechos digitales 55
Disposiciones adicionales 60

Disposiciones transitorias . . . 66
Disposiciones derogatorias . . . 68
Disposiciones finales . . . 68

§ 4. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal . . . 75

Preámbulo . . . 75
Artículos . . . 77
Disposiciones transitorias . . . 77
Disposiciones derogatorias . . . 78
Disposiciones finales . . . 79
REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL . . . 79
TÍTULO I. Disposiciones generales . . . 79
TÍTULO II. Principios de protección de datos . . . 83
CAPÍTULO I. Calidad de los datos . . . 83
CAPÍTULO II. Consentimiento para el tratamiento de los datos y deber de información . . . 85
Sección 1.ª Obtención del consentimiento del afectado . . . 85
Sección 2.ª Deber de información al interesado . . . 87
CAPÍTULO III. Encargado del tratamiento . . . 87
TÍTULO III. Derechos de acceso, rectificación, cancelación y oposición . . . 88
CAPÍTULO I. Disposiciones generales . . . 88
CAPÍTULO II. Derecho de acceso . . . 90
CAPÍTULO III. Derechos de rectificación y cancelación . . . 92
CAPÍTULO IV. Derecho de oposición . . . 92
TÍTULO IV. Disposiciones aplicables a determinados ficheros de titularidad privada . . . 93
CAPÍTULO I. Ficheros de información sobre solvencia patrimonial y crédito . . . 93
Sección 1.ª Disposiciones generales . . . 93
Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés . . . 94
CAPÍTULO II. Tratamientos para actividades de publicidad y prospección comercial . . . 96
TÍTULO V. Obligaciones previas al tratamiento de los datos . . . 99
CAPÍTULO I. Creación, modificación o supresión de ficheros de titularidad pública . . . 99
CAPÍTULO II. Notificación e inscripción de los ficheros de titularidad pública o privada . . . 100
TÍTULO VI. Transferencias internacionales de datos . . . 103
CAPÍTULO I. Disposiciones generales . . . 103
CAPÍTULO II. Transferencias a estados que proporcionen un nivel adecuado de protección . . . 103
CAPÍTULO III. Transferencias a Estados que no proporcionen un nivel adecuado de protección . . . 104
TÍTULO VII. Códigos tipo . . . 105
TÍTULO VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal . . . 108
CAPÍTULO I. Disposiciones generales . . . 108
CAPÍTULO II. Del documento de seguridad . . . 110
CAPÍTULO III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados . . . 111
Sección 1.ª Medidas de seguridad de nivel básico . . . 111
Sección 2.ª Medidas de seguridad de nivel medio . . . 113
Sección 3.ª Medidas de seguridad de nivel alto . . . 114
CAPÍTULO IV. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados . . . 115
Sección 1.ª Medidas de seguridad de nivel básico . . . 115
Sección 2.ª Medidas de seguridad de nivel medio . . . 116
Sección 3.ª Medidas de seguridad de nivel alto . . . 116
TÍTULO IX. Procedimientos tramitados por la Agencia Española de Protección de Datos . . . 117
CAPÍTULO I. Disposiciones generales . . . 117
CAPÍTULO II. Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición . . . 117
CAPÍTULO III. Procedimientos relativos al ejercicio de la potestad sancionadora . . . 118
Sección 1.ª Disposiciones generales . . . 118
Sección 2.ª Actuaciones previas . . . 119
Sección 3.ª Procedimiento sancionador . . . 120
Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas . . . 120
CAPÍTULO IV. Procedimientos relacionados con la inscripción o cancelación de ficheros . . . 121
Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros . . . 121
Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos . . . 122
CAPÍTULO V. Procedimientos relacionados con las transferencias internacionales de datos . . . 122

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos . . . 122
Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos . . . 123
CAPÍTULO VI. Procedimiento de inscripción de códigos tipo . . . 124
CAPÍTULO VII. Otros procedimientos tramitados por la agencia española de protección de datos . . . 125
Sección 1.ª Procedimiento de exención del deber de información al interesado . . . 125
Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos . . . 126
Disposiciones adicionales . . . 127
Disposiciones finales . . . 127

§ 5. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) . . . 128

Preámbulo . . . 128
CAPÍTULO I. Disposiciones generales . . . 163
CAPÍTULO II. Principios . . . 167
CAPÍTULO III. Derechos del interesado . . . 171
Sección 1. Transparencia y modalidades . . . 171
Sección 2. Información y acceso a los datos personales . . . 172
Sección 3. Rectificación y supresión . . . 174
Sección 4. Derecho de oposición y decisiones individuales automatizadas . . . 176
Sección 5. Limitaciones . . . 177
CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento . . . 178
Sección 1. Obligaciones generales . . . 178
Sección 2. Seguridad de los datos personales . . . 182
Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa . . . 183
Sección 4. Delegado de protección de datos . . . 185
Sección 5. Códigos de conducta y certificación . . . 187
CAPÍTULO V. Transferencias de datos personales a terceros países u organizaciones internacionales . . . 191
CAPÍTULO VI. Autoridades de control independientes . . . 196
Sección 1. Independencia . . . 196
Sección 2. Competencia, funciones y poderes . . . 197
CAPÍTULO VII. Cooperación y coherencia . . . 201
Sección 1. Cooperación y coherencia . . . 201
Sección 2. Coherencia . . . 204
Sección 3. Comité europeo de protección de datos . . . 206
CAPÍTULO VIII. Recursos, responsabilidad y sanciones . . . 210
CAPÍTULO IX. Disposiciones relativas a situaciones específicas de tratamiento . . . 213
CAPÍTULO X. Actos delegados y actos de ejecución . . . 215
CAPÍTULO XI. Disposiciones finales . . . 216

§ 6. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras . . . 218

Preámbulo . . . 218
Artículos . . . 220
Disposiciones transitorias . . . 221
Disposiciones finales . . . 221
ANEXO. 1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal . . . 221

§ 7. Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo . . . 223

Preámbulo . . . 223
Artículos . . . 223

§ 8. Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios 225

Preámbulo 225
Artículos 225

§ 9. Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal 227

Preámbulo 227
Artículos 227

§ 10. Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos 229

Preámbulo 229
CAPÍTULO I. Disposiciones generales 230
CAPÍTULO II. Organización 232
CAPÍTULO III. Relaciones con otros organismos e instituciones 235
CAPÍTULO IV. Ejercicio de competencias y funciones 236
CAPÍTULO V. Régimen jurídico, de personal, económico y de contratación 239
Disposiciones transitorias 240
Disposiciones derogatorias 241
Disposiciones finales 241

§ 11. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos 242

Preámbulo 242
TÍTULO I. Disposiciones generales 244
TÍTULO II. La Agencia Vasca de Protección de Datos 247
TÍTULO III. Régimen sancionador 251
Disposiciones adicionales 253
Disposiciones finales 254

SOCIEDAD DE LA INFORMACIÓN

§ 12. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico 255

Preámbulo 255
TÍTULO I. Disposiciones generales 258
CAPÍTULO I. Objeto 258
CAPÍTULO II. Ámbito de aplicación 258
TÍTULO II. Prestación de servicios de la sociedad de la información 260
CAPÍTULO I. Principio de libre prestación de servicios 260
CAPÍTULO II. Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información 261
Sección 1.ª Obligaciones 261
Sección 2.ª Régimen de responsabilidad 264
CAPÍTULO III. Códigos de conducta 266
TÍTULO III. Comunicaciones comerciales por vía electrónica 266
TÍTULO IV. Contratación por vía electrónica 268
TÍTULO V. Solución judicial y extrajudicial de conflictos 270
CAPÍTULO I. Acción de cesación 270
CAPÍTULO II. Solución extrajudicial de conflictos 270
TÍTULO VI. Información y control 271
TÍTULO VII. Infracciones y sanciones 272
Disposiciones adicionales 278
Disposiciones transitorias 283
Disposiciones finales 283

ANEXO. Definiciones . . . 286

§ 13. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información . . . 289

Preámbulo . . . 289
CAPÍTULO I. Medidas de impulso de la sociedad de la información . . . 297
CAPÍTULO II. Modificaciones legislativas para el impulso de la sociedad de la información y de las comunicaciones electrónicas . . . 301
Disposiciones adicionales . . . 311
Disposiciones transitorias . . . 319
Disposiciones finales . . . 319

NORMATIVA CONEXA

CIVIL

§ 14. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. . . . 321

Preámbulo . . . 321
CAPITULO I. Disposiciones generales . . . 323
CAPITULO II. De la protección civil del honor, de la intimidad y de la propia imagen . . . 324
DISPOSICIÓN DEROGATORIA. . . . 325
DISPOSICIONES TRANSITORIAS . . . 326

§ 15. Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación. . . . 327

Preámbulo . . . 327
Artículos . . . 327
Disposiciones derogatorias . . . 329

§ 16. Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. [Inclusión parcial] . . 330

[. . .]

TÍTULO PRELIMINAR. De las normas jurídicas, su aplicación y eficacia. . . . 330

[. . .]

CAPÍTULO III. Eficacia general de las normas jurídicas. . . . 330

[. . .]

LIBRO CUARTO. De las obligaciones y contratos . . . 331
TÍTULO I. De las obligaciones . . . 331

[. . .]

CAPÍTULO II. De la naturaleza y efecto de las obligaciones . . . 331
TÍTULO XVI. De las obligaciones que se contraen sin convenio . . . 331

[. . .]

CAPÍTULO II. De las obligaciones que nacen de culpa o negligencia . . . 331

§ 17. Ley 20/2011, de 21 de julio, del Registro Civil . . . 332

Preámbulo . . . 332
TÍTULO I. El Registro Civil. Disposiciones generales . . . 336
CAPÍTULO PRIMERO. Naturaleza, contenido y competencias del Registro Civil . . . 336
CAPÍTULO SEGUNDO. Derechos y deberes ante el Registro Civil . . . 338
TÍTULO II. Principios de funcionamiento del Registro Civil. . . . 339
TÍTULO III. Estructura y dependencia del Registro Civil . . . 340
CAPÍTULO PRIMERO. Oficinas del Registro Civil . . . 340
CAPÍTULO SEGUNDO. La Dirección General de los Registros y del Notariado . . . 342
TÍTULO IV. Títulos que acceden al Registro Civil. Control de legalidad . . . 342
CAPÍTULO PRIMERO. Títulos que acceden al Registro Civil . . . 342

CAPÍTULO SEGUNDO. Control de legalidad . . . 343
TÍTULO V. Los asientos registrales . . . 344
CAPÍTULO PRIMERO. Competencia para efectuar los asientos . . . 344
CAPÍTULO SEGUNDO. Reglas generales para la práctica de asientos . . . 344
CAPÍTULO TERCERO. Clases de asientos . . . 345
CAPÍTULO CUARTO. Promoción de la inscripción y de otros asientos . . . 345
TÍTULO VI. Hechos y actos inscribibles . . . 346
CAPÍTULO PRIMERO. Inscripción de nacimiento . . . 346
Sección 1.ª Hecho inscribible y personas obligadas a promover la inscripción . . . 346
Sección 2.ª Contenido de la inscripción de nacimiento . . . 349
CAPÍTULO SEGUNDO. Inscripciones relativas al matrimonio . . . 351
CAPÍTULO TERCERO. Inscripción de la defunción . . . 355
CAPÍTULO CUARTO. Otras inscripciones . . . 356
CAPÍTULO QUINTO. Inscripciones en circunstancias excepcionales . . . 359
TÍTULO VII. Publicidad del Registro Civil . . . 359
CAPÍTULO PRIMERO. Instrumentos de publicidad registral . . . 359
CAPÍTULO SEGUNDO. Datos sometidos a régimen de protección especial . . . 360
TÍTULO VIII. Régimen de recursos . . . 361
TÍTULO IX. Los procedimientos registrales . . . 362
CAPÍTULO PRIMERO. Reglas generales de los procedimientos registrales . . . 362
CAPÍTULO SEGUNDO. Rectificación de los asientos del Registro Civil . . . 363
CAPÍTULO TERCERO. Declaraciones con valor de simple presunción . . . 363
TÍTULO X. Normas de Derecho internacional privado . . . 364
Disposiciones adicionales . . . 366
Disposiciones transitorias . . . 368
Disposiciones derogatorias . . . 371
Disposiciones finales . . . 372

§ 18. Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención relativa al sexo de las personas . . . 375

Preámbulo . . . 375
Artículos . . . 376
Disposiciones adicionales . . . 377
Disposiciones transitorias . . . 378
Disposiciones finales . . . 378

PENAL

§ 19. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial] . . . 379

[. . .]

TÍTULO VII. De la extinción de la responsabilidad criminal y sus efectos . . . 379

[. . .]

CAPÍTULO II. De la cancelación de antecedentes delictivos . . . 379
TÍTULO VI. Delitos contra la libertad . . . 380

[. . .]

CAPÍTULO II. De las amenazas . . . 380

[. . .]

TÍTULO VII. De las torturas y otros delitos contra la integridad moral . . . 381
TÍTULO VIII. Delitos contra la libertad e indemnidad sexuales . . . 382

[. . .]

CAPÍTULO V. De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores . . . 382
TÍTULO X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio . . . 384
CAPÍTULO I. Del descubrimiento y revelación de secretos . . . 384

[. . .]

TÍTULO XI. Delitos contra el honor . . . 386

CAPÍTULO I. De la calumnia . . . 386
CAPÍTULO II. De la injuria . . . 386
CAPÍTULO III. Disposiciones generales . . . 387

[. . .]

Sección 2.ª bis De la apropiación indebida . . . 387

ADMINISTRACIÓN DE JUSTICIA

§ 20. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial] . . . 388

[. . .]

LIBRO III. DEL RÉGIMEN DE LOS JUZGADOS Y TRIBUNALES . . . 388

[. . .]

TÍTULO III. De las actuaciones judiciales . . . 388

[. . .]

CAPÍTULO V. De la vista, votación y fallo . . . 388

[. . .]

LIBRO VIII. Del Consejo General del Poder Judicial . . . 389
TÍTULO I. De las atribuciones del Consejo General del Poder Judicial . . . 389

§ 21. Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional . . . 392

Preámbulo . . . 392
TÍTULO I. Del Tribunal Constitucional . . . 392
CAPÍTULO I. Del Tribunal Constitucional, su organización y atribuciones . . . 392
CAPÍTULO II. De los Magistrados del Tribunal Constitucional . . . 395
TÍTULO II. De los procedimientos de declaración de inconstitucionalidad . . . 397
CAPÍTULO I. Disposiciones generales . . . 397
CAPÍTULO II. Del recurso de inconstitucionalidad . . . 398
CAPÍTULO III. De la cuestión de inconstitucionalidad promovida por Jueces o Tribunales . . . 399
CAPÍTULO IV. De la sentencia en procedimientos de inconstitucionalidad y de sus efectos . . . 400
TÍTULO III. Del recurso de amparo constitucional . . . 401
CAPÍTULO I. De la procedencia e interposición del recurso de amparo constitucional . . . 401
CAPÍTULO II. De la tramitación de los recursos de amparo constitucional . . . 403
CAPÍTULO III. De la resolución de los recursos de amparo constitucional y sus efectos . . . 404
TÍTULO IV. De los conflictos constitucionales . . . 405
CAPÍTULO I. Disposiciones generales . . . 405
CAPÍTULO II. De los conflictos entre el Estado y las Comunidades Autónomas o de éstas entre sí . . . 406
Sección primera. Conflictos positivos . . . 406
Sección segunda. Conflictos negativos . . . 408
CAPÍTULO III. De los conflictos entre órganos constitucionales del Estado . . . 409
CAPÍTULO IV. De los conflictos en defensa de la autonomía local . . . 410
TÍTULO V. De la impugnación de disposiciones sin fuerza de Ley y resoluciones de las Comunidades Autónomas prevista en el artículo 161.2 de la Constitución . . . 411
TÍTULO VI. De la declaración sobre la constitucionalidad de los tratados internacionales . . . 411
TÍTULO VI BIS.. Del recurso previo de inconstitucionalidad contra Proyectos de Estatutos de Autonomía y contra Propuestas de Reforma de Estatutos de Autonomía . . . 412
TÍTULO VII. De las disposiciones comunes sobre procedimiento . . . 412
TÍTULO VIII. Del personal al servicio del Tribunal Constitucional . . . 416
DISPOSICIONES TRANSITORIAS . . . 417
DISPOSICIONES ADICIONALES . . . 418

§ 22. Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia . . . 420

Preámbulo . . . 420
TÍTULO I. Del ámbito de aplicación y los principios generales . . . 424
TÍTULO II. Uso de los medios electrónicos en la Administración de Justicia . . . 425

CAPÍTULO I. Derechos de los ciudadanos en sus relaciones con la Administración de Justicia por medios electrónicos . . . 425
CAPÍTULO II. Derechos y deberes de los profesionales de la justicia en sus relaciones con la Administración de Justicia por medios electrónicos . . . 426
CAPÍTULO III. Utilización obligatoria de los medios electrónicos en la tramitación de los procedimientos electrónicos judiciales . . . 427
TÍTULO III. Régimen jurídico de la Administración judicial electrónica . . . 427
CAPÍTULO I. De la sede judicial electrónica . . . 427
CAPÍTULO II. De la identificación y autenticación . . . 429
Sección 1.ª Disposiciones comunes . . . 429
Sección 2.ª Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia. . . . 430
Sección 3.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos . . . 432
TÍTULO IV. De la tramitación electrónica de los procedimientos judiciales . . . 433
CAPÍTULO I. Disposiciones comunes . . . 433
CAPÍTULO II. Del expediente judicial electrónico . . . 433
CAPÍTULO III. Del registro de escritos, las comunicaciones y las notificaciones electrónicas . . . 435
Sección 1.ª Del registro de escritos . . . 435
Sección 2.ª De las comunicaciones y las notificaciones electrónicas . . . 437
CAPÍTULO IV. De la tramitación electrónica . . . 438
TÍTULO V. Cooperación entre las Administraciones con competencias en materia de Administración de Justicia. El Esquema judicial de interoperabilidad y seguridad . . . 440
CAPÍTULO I. Marco institucional de cooperación en materia de administración electrónica . . . 440
CAPÍTULO II. Esquema judicial de interoperabilidad y seguridad . . . 441
Sección 1.ª Interoperabilidad judicial . . . 441
Sección 2.ª Seguridad judicial electrónica . . . 442
CAPÍTULO III. Reutilización de aplicaciones y transferencia de tecnologías. Directorio general de información tecnológica judicial . . . 443
Disposiciones adicionales . . . 444
Disposiciones transitorias . . . 446
Disposiciones finales . . . 446
ANEXO. Definiciones . . . 446

§ 23. Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia . . . 450

Preámbulo . . . 450
CAPÍTULO I. Disposiciones generales . . . 452
CAPÍTULO II. Acceso a la información . . . 454
CAPÍTULO III. Información contenida en el sistema . . . 456
CAPÍTULO IV. Medidas de seguridad . . . 458
CAPÍTULO V. Certificación de los datos . . . 458
CAPÍTULO VI. Cancelación o rectificación de inscripciones . . . 460
Disposiciones adicionales . . . 462
Disposiciones transitorias . . . 463
Disposiciones derogatorias . . . 463
Disposiciones finales . . . 464

ADMINISTRACIONES PÚBLICAS

§ 24. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial] . . . 465

[. . .]

TÍTULO II. De la actividad de las Administraciones Públicas . . . 465
CAPÍTULO I. Normas generales de actuación . . . 465
TÍTULO III. De los actos administrativos . . . 466

[. . .]

CAPÍTULO II. Eficacia de los actos. . . . 466
CAPÍTULO III. Nulidad y anulabilidad . . . 469

[. . .]

§ 25. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. [Inclusión parcial] 471

Preámbulo 471
Artículos 476
Disposiciones transitorias 476
Disposiciones derogatorias 477
Disposiciones finales 477
REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS 478
TÍTULO PRELIMINAR. Disposiciones generales 478
TÍTULO I. Portales de internet, Punto de Acceso General electrónico y sedes electrónicas 480
TÍTULO II. Procedimiento administrativo por medios electrónicos 484
CAPÍTULO I. Disposiciones generales 484
CAPÍTULO II. De la identificación y autenticación de las Administraciones Públicas y las personas interesadas 485
Sección 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad . . . 485
Sección 2.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia 486
Sección 3.ª Identificación y firma de las personas interesadas 490
Sección 4.ª Acreditación de la representación de las personas interesadas 493
CAPÍTULO III. Registros, comunicaciones y notificaciones electrónicas 496
Sección 1.ª Registros electrónicos 496
Sección 2.ª Comunicaciones y notificaciones electrónicas 498
TÍTULO III. Expediente administrativo electrónico 502
CAPÍTULO I. Documento administrativo electrónico y copias 502
CAPÍTULO II. Archivo electrónico de documentos 504
TÍTULO IV. De las relaciones y colaboración entre las Administraciones Públicas para el funcionamiento del sector público por medios electrónicos 505
CAPÍTULO I. Colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos 505
CAPÍTULO II. Transferencia y uso compartido de tecnologías entre Administraciones Públicas 508
Disposiciones adicionales 510
ANEXO. Definiciones 513

§ 26. Ley 9/1968, de 5 de abril, sobre secretos oficiales 517

Preámbulo 517
Artículos 518
DISPOSICIÓN FINAL 520

§ 27. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica 521

Preámbulo 521
CAPÍTULO I. Disposiciones generales 523
CAPÍTULO II. Principios básicos 524
CAPÍTULO III. Interoperabilidad organizativa 524
CAPÍTULO IV. Interoperabilidad semántica 525
CAPÍTULO V. Interoperabilidad técnica 526
CAPÍTULO VI. Infraestructuras y servicios comunes 527
CAPÍTULO VII. Comunicaciones de las Administraciones públicas 527
CAPÍTULO VIII. Reutilización y transferencia de tecnología 528
CAPÍTULO IX. Firma electrónica y certificados 529
CAPÍTULO X. Recuperación y conservación del documento electrónico 530
CAPÍTULO XI. Normas de conformidad 532
CAPÍTULO XII. Actualización 533
Disposiciones adicionales 533
Disposiciones transitorias 536
Disposiciones derogatorias 536
Disposiciones finales 536
ANEXO. Glosario de términos 536

§ 28. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica . . . 540

Preámbulo . . . 540
CAPÍTULO I. Disposiciones generales . . . 542
CAPÍTULO II. Principios básicos . . . 543
CAPÍTULO III. Requisitos mínimos . . . 544
CAPÍTULO IV. Comunicaciones electrónicas . . . 549
CAPÍTULO V. Auditoría de la seguridad . . . 549
CAPITULO VI. Estado de seguridad de los sistemas . . . 550
CAPÍTULO VII. Respuesta a incidentes de seguridad . . . 550
CAPÍTULO VIII. Normas de conformidad . . . 551
CAPÍTULO IX. Actualización . . . 552
CAPÍTULO X. Categorización de los sistemas de información . . . 552
Disposiciones adicionales . . . 552
Disposiciones transitorias . . . 553
Disposiciones derogatorias . . . 553
Disposiciones finales . . . 554
ANEXOS . . . 554
ANEXO I. Categorías de los sistemas . . . 554
ANEXO II. Medidas de seguridad . . . 556
ANEXO III. Auditoría de la seguridad . . . 585
ANEXO IV. Glosario . . . 586
ANEXO V. Modelo de cláusula administrativa particular . . . 587

MENORES

§ 29. Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil . . . 588

Preámbulo . . . 588
TÍTULO I. De los derechos y deberes de los menores . . . 593
CAPÍTULO I. Ámbito e interés superior del menor . . . 593
CAPÍTULO II. Derechos del menor . . . 595
CAPÍTULO III. Deberes del menor . . . 598
CAPÍTULO IV. Medidas y principios rectores de la acción administrativa . . . 599
TÍTULO II. Actuaciones en situación de desprotección social del menor e instituciones de protección de menores 601
CAPÍTULO I. Actuaciones en situaciones de desprotección social del menor . . . 601
CAPÍTULO II. De la tutela . . . 615
CAPÍTULO III. De la adopción . . . 616
CAPÍTULO IV. Centros de protección específicos de menores con problemas de conducta . . . 616
Disposiciones adicionales . . . 620
Disposiciones transitorias . . . 620
Disposiciones derogatorias . . . 620
Disposiciones finales . . . 620

SANITARIA

§ 30. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica . . . 631

Preámbulo . . . 631
CAPÍTULO I. Principios generales . . . 633
CAPÍTULO II. El derecho de información sanitaria . . . 634
CAPÍTULO III. Derecho a la intimidad . . . 635
CAPÍTULO IV. El respeto de la autonomía del paciente . . . 635
CAPÍTULO V. La historia clínica . . . 638
CAPÍTULO VI. Informe de alta y otra documentación clínica . . . 641
Disposiciones adicionales . . . 641
Disposiciones transitorias . . . 642
Disposiciones derogatorias . . . 642

Disposiciones finales 642

BOLETINES OFICIALES

§ 31. Ley 5/2002, de 4 de abril, reguladora de los Boletines Oficiales de las Provincias 643

Preámbulo 643
CAPÍTULO I. El Boletín Oficial de la Provincia. 645
CAPÍTULO II. Régimen económico del Boletín Oficial de la Provincia 647
Disposiciones adicionales 648
Disposiciones transitorias 649
Disposiciones derogatorias 649
Disposiciones finales 649

§ 32. Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado» 650

Preámbulo 650
CAPÍTULO I. Disposiciones generales 651
CAPÍTULO II. Contenido del «Boletín Oficial del Estado» 652
CAPÍTULO III. Edición electrónica 654
CAPÍTULO IV. Acceso de los ciudadanos al «Boletín Oficial del Estado». 655
CAPÍTULO V. Procedimiento de publicación 656
Disposiciones adicionales 659
Disposiciones transitorias 661
Disposiciones derogatorias 661
Disposiciones finales 661
ANEXO I. Formato XML para el envío de anuncios de notificación 662
ANEXO II. Formato XML para el envío de los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único 666

INDULTOS

§ 33. Ley de 18 de junio de 1870 estableciendo reglas para el ejercicio de la gracia de indulto. 669

CAPÍTULO I. De los que pueden ser indultados 669
CAPÍTULO II. De las clases y efectos del indulto 669
CAPÍTULO III. Del procedimiento para solicitar y conceder la gracia del indulto 671
Disposiciones adicionales 673

FUERZAS Y CUERPOS DE SEGURIDAD

§ 34. Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. [Inclusión parcial] 674

TÍTULO I. De los Cuerpos y Fuerzas de Seguridad 674

[. . .]

CAPÍTULO II. Principios básicos de actuación 674

[. . .]

[. . .]

[. . .]

§ 35. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN 676

Preámbulo 676
Artículos 678

§ 36. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos . . . 682

Preámbulo . . . 682
Artículos . . . 683
Disposiciones adicionales . . . 686
Disposiciones transitorias . . . 688
Disposiciones finales . . . 688

§ 37. Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. [Inclusión parcial] . . . 689

[. . .]

CAPÍTULO II. Documentación e identificación personal . . . 689
CAPÍTULO III. Actuaciones para el mantenimiento y restablecimiento de la seguridad ciudadana . . . 690
Sección 1.ª Potestades generales de policía de seguridad . . . 690
CAPÍTULO IV. Potestades especiales de policía administrativa de seguridad . . . 691

§ 38. Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas. [Inclusión parcial] . . . 692

Capítulo preliminar. Disposiciones generales . . . 692

[. . .]

[. . .]

Capítulo III. Medidas de seguridad en fabricación, circulación y comercio . . . 693

[. . .]

Capítulo V. Licencias, autorizaciones especiales y tarjetas de armas . . . 693
Sección 1. Licencias en general y tarjetas . . . 693

[. . .]

Aptitudes físicas y psíquicas . . . 693
Expedición de licencias B, D y E a particulares . . . 694
Tarjetas . . . 694

[. . .]

Armas antiguas, históricas y artísticas. Armas de avancarga y de sistema «Flobert». Armas acústicas y de salvas. Armas inutilizadas . . . 695

[. . .]

Capítulo VI. Tenencia y uso de armas de concurso . . . 696
INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 1. Características y medidas de seguridad en galerías y campos de tiro . . . 696
INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 2. Normas y técnicas de inutilización de las armas de fuego para garantizar que las armas de fuego inutilizadas lo sean irreversiblemente . . . 701
ANEXO I. Especificaciones técnicas para la inutilización de armas de fuego . . . 703
ANEXO II. Modelo de marcado de armas de fuego inutilizadas . . . 709
ANEXO III. Modelo de certificado para armas inutilizadas . . . 710
INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 3. Armas de alarma y señales . . . 710
ANEXO. Especificaciones técnicas de las armas de alarma y señales . . . 711
INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 4. Especificaciones técnicas de marcado de las armas y los componentes esenciales . . . 712
INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 5. Tarjeta Europea de Armas de Fuego . . . 713
ANEXO I . . . 714
ANEXO II . . . 716

§ 39. Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior. . . . 717

Preámbulo . . . 717

Artículos . . . 718
Disposiciones adicionales . . . 718
Disposiciones transitorias . . . 718
Disposiciones derogatorias . . . 718
Disposiciones finales . . . 719
ANEXO I . . . 719
ANEXO II . . . 762
ANEXO III . . . 919

NORMATIVA PENITENCIARIA

§ 40. Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario. [Inclusión parcial] . . . 923

REGLAMENTO PENITENCIARIO . . . 923
TITULO I. Disposiciones generales . . . 923

[. . .]

CAPITULO II. De los derechos y deberes de los internos . . . 923
CAPITULO III. Protección de los datos de carácter personal de los ficheros penitenciarios . . . 924
TITULO X. Del régimen disciplinario y de las recompensas . . . 924

[. . .]

CAPITULO V. Prescripción y cancelación . . . 924

[. . .]

TELECOMUNICACIONES

§ 41. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones . . . 926

Preámbulo . . . 926
CAPÍTULO I. Disposiciones generales . . . 928
CAPÍTULO II. Conservación y cesión de datos . . . 930
CAPÍTULO III. Infracciones y sanciones . . . 932
Disposiciones adicionales . . . 932
Disposiciones transitorias . . . 933
Disposiciones derogatorias . . . 933
Disposiciones finales . . . 934

§ 42. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial] . . . 937

[. . .]

TÍTULO III. Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas . . . 937

[. . .]

CAPÍTULO III. Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas . . . 937
CAPÍTULO IV. Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios . . . 939

§ 43. Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas . . . 941

Preámbulo . . . 941
TÍTULO I. DISPOSICIONES GENERALES . . . 943
TÍTULO II. CARTA DE DERECHOS DEL USUARIO DE LOS SERVICIOS DE COMUNICACIONES ELECTRÓNICAS . . . 944

CAPÍTULO I. Derecho al acceso a la red telefónica fija, con una conexión que garantice el acceso funcional a Internet, así como al resto de prestaciones incluidas en el servicio universal, a un precio asequible y con una calidad determinada . . . 945
CAPÍTULO II. Derecho a celebrar contratos y a rescindirlos, así como a cambiar de operador . . . 945
CAPÍTULO III. Derecho a la información veraz, eficaz, suficiente, transparente y actualizada sobre las concisiones ofrecidas por los operadores y las garantías legales . . . 949
CAPÍTULO IV. Derecho a recibir servicios de telecomunicaciones con garantías de calidad, así como a recibir información comparable, pertinente y actualizada sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público . . . 950
CAPÍTULO V. Derecho a la continuidad del servicio y a ser indemnizado en caso de Interrupción . . . 950
CAPÍTULO VI. Derecho a la facturación desglosada, a la desconexión de determinados servicios y a elegir el medio de pago de los servicios entre los comúnmente utilizados en el tráfico comercial. . . . 953
CAPÍTULO VII. Derecho a una atención eficaz por el operador . . . 955
CAPÍTULO VIII. Derecho a vías rápidas y eficaces para reclamar . . . 956
CAPÍTULO IX. Derecho a prestaciones especiales para personas con discapacidad y de renta baja . . . 956
CAPÍTULO X. Protección en la utilización de servicios de tarificación adicional . . . 957
CAPÍTULO XI. Derecho a la protección de los datos personales . . . 958
CAPÍTULO XII. Obligaciones de los usuarios finales. . . . 958
Disposiciones transitorias . . . 959
Disposiciones derogatorias . . . 959
Disposiciones finales . . . 959

CONSUMIDORES Y USUARIOS

§ 44. Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. [Inclusión parcial] . . . 961

LIBRO PRIMERO. Disposiciones generales. . . . 961
TÍTULO I. Ámbito de aplicación y derechos básicos de los consumidores y usuarios . . . 961

[. . .]

CAPÍTULO II. Derechos básicos de los consumidores y usuarios . . . 961
TÍTULO III. Contratos celebrados a distancia y contratos celebrados fuera del establecimiento mercantil . . . 962
CAPÍTULO I. Disposiciones generales . . . 962

[. . .]

§ 45. Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. . . . 964

Preámbulo . . . 964
Artículos . . . 966
Disposiciones adicionales . . . 966
Disposiciones transitorias . . . 966
Disposiciones derogatorias . . . 967
Disposiciones finales . . . 967
REGLAMENTO SOBRE LAS CONDICIONES PARA LA PRESTACIÓN DE SERVICIOS DE COMUNICACIONES ELECTRÓNICAS, EL SERVICIO UNIVERSAL Y LA PROTECCIÓN DE LOS USUARIOS . . . 980
TÍTULO I. Disposiciones generales . . . 980
TÍTULO II. Explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia . . . 981
CAPÍTULO I. Régimen general de explotación de redes y de prestación de servicios de comunicaciones electrónicas . . . 981
CAPÍTULO II. Registro de operadores. . . . 983
CAPÍTULO III. Condiciones para la explotación de redes y la prestación de servicios de comunicaciones electrónicas . . . 986
TÍTULO III. Obligaciones de servicio público y de carácter público . . . 990
CAPÍTULO I. Disposiciones generales . . . 990
CAPÍTULO II. Servicio universal . . . 991
Sección 1.ª Delimitación del servicio universal . . . 991
Sección 2.ª Carácter asequible del precio del servicio universal . . . 998

Sección 3.ª Operadores obligados a la prestación. Procedimiento de designación de operadores 1000
Sección 4.ª Coste neto de la prestación del servicio universal 1002
Sección 5.ª Financiación del servicio universal. 1004
CAPÍTULO III. Otras obligaciones de servicio público 1007
TÍTULO IV. Derecho de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y condiciones de establecimiento de servidumbres y limitaciones 1009
TÍTULO V. Obligaciones de carácter público. Secreto de las comunicaciones y protección de los datos personales 1010
CAPÍTULO I. Protección de los datos personales en la explotación de redes y en la prestación de los servicios de comunicaciones electrónicas disponibles al público. 1010
Sección 1.ª Disposiciones generales 1010
Sección 2.ª Los datos de carácter personal en relación con determinados aspectos de los servicios de comunicaciones electrónicas 1012
Sección 3.ª Protección de los datos personales en los servicios avanzados de telefonía 1016
CAPÍTULO II. La interceptación legal de las comunicaciones 1019
Sección 1.ª Disposiciones generales 1019
Sección 2.ª Requisitos operacionales 1021
TÍTULO VI. Derechos de los consumidores que sean personas físicas y otros usuarios finales 1024
CAPÍTULO I. Disposiciones generales 1024
CAPÍTULO II. Contratos 1024
CAPÍTULO III. Derechos y obligaciones de transparencia, información y calidad 1024
CAPÍTULO IV. Derechos en relación con el servicio telefónico disponible al público 1024
CAPÍTULO V. Derechos en relación con el servicio de acceso a Internet 1024
Disposiciones adicionales 1024
Disposiciones transitorias 1025
Disposiciones finales 1027

NORMATIVA TRIBUTARIA

§ 46. Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial] 1028

[. . .]

TÍTULO III. La aplicación de los tributos 1028
CAPÍTULO I. Principios generales 1028

[. . .]

Sección 3.ª Colaboración social en la aplicación de los tributos 1028
Sección 4.ª Tecnologías informáticas y telemáticas 1033
CAPÍTULO II. Normas comunes sobre actuaciones y procedimientos tributarios 1034
Sección 1.ª Especialidades de los procedimientos administrativos en materia tributaria 1034
Subsección 1.ª Fases de los procedimientos tributarios 1034
Sección 3.ª Notificaciones. 1035

[. . .]

§ 47. Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos. [Inclusión parcial]. . . . 1036

TÍTULO II. Las obligaciones tributarias formales 1036
CAPÍTULO I. Las obligaciones censales 1036

[. . .]

[. . .]

Subsección 2.ª Las declaraciones censales en el ámbito de competencias del Estado 1037
TÍTULO III. Principios y disposiciones generales de la aplicación de los tributos 1040

[. . .]

CAPÍTULO II. Principios generales de la aplicación de los tributos 1040

[. . .]

Sección 2.ª La colaboración social en la aplicación de los tributos 1041

CAPÍTULO III. Normas comunes sobre actuaciones y procedimientos tributarios 1041
Sección 1.ª Especialidades de los procedimientos administrativos en materia tributaria 1041

[. . .]

Subsección 2.ª Tramitación de las actuaciones y procedimientos tributarios 1041

SEGURIDAD SOCIAL

§ 48. Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social. [Inclusión parcial]. 1042

TÍTULO I. Normas generales del sistema de la Seguridad Social 1042

[. . .]

CAPÍTULO III. Afiliación, cotización y recaudación 1042

[. . .]

Sección 3.ª Liquidación y recaudación de las cuotas y demás recursos del sistema 1042

[. . .]

Subsección 3.ª Recaudación en vía ejecutiva 1042
CAPÍTULO IV. Acción protectora 1044

[. . .]

Sección 3.ª Prescripción, caducidad y reintegro de prestaciones indebidas 1044
Subsección 2.ª Pensiones contributivas 1044
CAPÍTULO V. Gestión de la Seguridad Social 1046
Sección 1.ª Entidades gestoras 1046
Sección 3.ª Normas comunes a las entidades gestoras y servicios comunes 1049

PUBLICACIÓN DE SANCIONES DE TRÁFICO

§ 49. Orden INT/3022/2010, de 23 de noviembre, por la que se regula el Tablón Edictal de Sanciones de Tráfico 1052

Preámbulo 1052
Artículos 1053
Disposiciones adicionales 1057
Disposiciones transitorias 1058
Disposiciones derogatorias 1058
Disposiciones finales 1058

§ 1

Nota del autor

Última modificación: 22 de septiembre de 2014

La eliminación o el bloqueo de datos en internet y en buscadores web, la cancelación de antecedentes, la salida de ficheros de morosos y de listados comerciales, son algunas de las preocupaciones del ciudadano de hoy, y que busca resolver el llamado derecho al olvido. Este derecho, contemplado desde distintas perspectivas jurídicas (penal, civil, administrativa..), puede definirse como el derecho a salvaguardar la reputación, o procurar la tranquilidad de las personas, desligándolas de acontecimientos que les afecten.

Dispone la Constitución Española, en su artículo 18, que la Ley *limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos* y, en su artículo 20.4, que las libertades de expresión e información tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollan y, especialmente, en el derecho al honor, a la intimidad y a la propia imagen.

En términos del propio Tribunal Constitucional, la redacción del artículo 18 expresado revela que el constituyente era consciente *de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, pero que es también, en sí mismo, un derecho o libertad fundamental"* (STC 254/1993, de 20 de julio, FJ 6).

La protección de los derechos fundamentales en la red es cada día más necesaria. La sociedad de la información, basada cada vez en mayor medida en internet, posibilita que cualquier contenido (aún perjudicial, inexacto u obsoleto), pueda ser objeto de una divulgación desproporcionada, accediéndose al mismo casi de forma inmediata a través de distintas plataformas (como los buscadores o redes sociales).

En este ámbito el llamado "derecho al olvido", también denominado "derecho a vivir en paz", se ha convertido en una pieza clave para la defensa de las personas, ya sean anónimas o públicas.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, dispuso en sus artículos 6.1.c, 12 y 14, que los datos objeto de tratamiento no podrían ser excesivos, debiendo suprimirse, rectificarse o bloquearse aquellos que fuesen inexactos o incompletos, y que a los particulares se les garantizaría la facultad para oponerse al tratamiento. Esta directiva configuró el espíritu de lo que hoy se denomina "derecho al olvido".

No existe sin embargo, una regulación concreta del "derecho al olvido". Cierta parte de la doctrina ha venido usando dicho término para referirse a otros derechos específicos, recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que se ejercitan para lograr la retirada o el bloqueo de datos personales

generalmente en internet, o el cese de un determinado tratamiento, como por ejemplo el referido a la cancelación de antecedentes penales y policiales, así como la oposición a prácticas comerciales o publicitarias.

Respondiendo a la falta de regulación concreta, el artículo 17 del Proyecto de Reforma del Reglamento del Parlamento Europeo y del Consejo (relativo a la protección y circulación de datos personales), regula concretamente el "derecho al olvido" y cabe esperar que esta nueva ordenación dote de mayor seguridad jurídica a los distintos operadores en lo referente a la protección de datos de carácter personal.

Al margen de la normativa de protección de datos (aplicable exclusivamente a datos de personas físicas), la mención del "derecho al olvido" se ha usado en la jurisdicción civil por aplicación de la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y de los preceptos que regulan la responsabilidad contractual y extracontractual.

El "derecho al olvido" tiene, además, un innegable carácter transversal. No sólo puede constituir per se el objeto de un litigio, sino que su invocación y correcto ejercicio puede servir además, en todos los ámbitos jurisdiccionales y en procedimientos de distinta naturaleza, de fundamento para la adopción de medidas cautelares, cesación de las injerencias efectuadas y la reparación integral de los perjuicios sufridos.

No ocultamos que el "derecho al olvido" es ampliamente debatido, bien por los grandes operadores de internet (buscadores y redes sociales), bien por parte de la doctrina jurídica que afirma que, en puridad, no cabe hablar de "derecho al olvido", cuando aún no se contempla como tal en el ordenamiento jurídico español el citado derecho. Sin embargo, el término "derecho al olvido" (con independencia de su regulación europea en materia de protección de datos) cabe aceptarse como una referencia comprensible de diferentes acciones jurídicas concretas, destinadas a proteger a las personas, generalmente, en la red.

Este código pretende hacer una recopilación de las principales normas referentes al llamado "derecho al olvido", teniendo en cuenta los diferentes ámbitos en los que se puede plantear.

Luis Gervas de la Pisa
VIDAU ABOGADOS

§ 2

Constitución Española. [Inclusión parcial]

Cortes Generales
«BOE» núm. 311, de 29 de diciembre de 1978
Última modificación: 27 de septiembre de 2011
Referencia: BOE-A-1978-31229

[. . .]

TÍTULO I

De los derechos y deberes fundamentales

Artículo 10.

1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

CAPÍTULO PRIMERO

De los españoles y los extranjeros

Artículo 11.

1. La nacionalidad española se adquiere, se conserva y se pierde de acuerdo con lo establecido por la ley.

2. Ningún español de origen podrá ser privado de su nacionalidad.

3. El Estado podrá concertar tratados de doble nacionalidad con los países iberoamericanos o con aquellos que hayan tenido o tengan una particular vinculación con España. En estos mismos países, aun cuando no reconozcan a sus ciudadanos un derecho recíproco, podrán naturalizarse los españoles sin perder su nacionalidad de origen.

Artículo 12.

Los españoles son mayores de edad a los dieciocho años.

Artículo 13.

1. Los extranjeros gozarán en España de las libertades públicas que garantiza el presente Título en los términos que establezcan los tratados y la ley.

2. Solamente los españoles serán titulares de los derechos reconocidos en el artículo 23, salvo lo que, atendiendo a criterios de reciprocidad, pueda establecerse por tratado o ley para el derecho de sufragio activo y pasivo en las elecciones municipales.

3. La extradición sólo se concederá en cumplimiento de un tratado o de la ley, atendiendo al principio de reciprocidad. Quedan excluidos de la extradición los delitos políticos, no considerándose como tales los actos de terrorismo.

4. La ley establecerá los términos en que los ciudadanos de otros países y los apátridas podrán gozar del derecho de asilo en España.

CAPÍTULO SEGUNDO

Derechos y libertades

Artículo 14.

Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social.

Sección 1.ª De los derechos fundamentales y de las libertades públicas

Artículo 15.

Todos tienen derecho a la vida y a la integridad física y moral, sin que, en ningún caso, puedan ser sometidos a tortura ni a penas o tratos inhumanos o degradantes. Queda abolida la pena de muerte, salvo lo que puedan disponer las leyes penales militares para tiempos de guerra.

Artículo 16.

1. Se garantiza la libertad ideológica, religiosa y de culto de los individuos y las comunidades sin más limitación, en sus manifestaciones, que la necesaria para el mantenimiento del orden público protegido por la ley.

2. Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

3. Ninguna confesión tendrá carácter estatal. Los poderes públicos tendrán en cuenta las creencias religiosas de la sociedad española y mantendrán las consiguientes relaciones de cooperación con la Iglesia Católica y las demás confesiones.

Artículo 17.

1. Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley.

2. La detención preventiva no podrá durar más del tiempo estrictamente necesario para la realización de las averiguaciones tendentes al esclarecimiento de los hechos, y, en todo caso, en el plazo máximo de setenta y dos horas, el detenido deberá ser puesto en libertad o a disposición de la autoridad judicial.

3. Toda persona detenida debe ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca.

4. La ley regulará un procedimiento de «habeas corpus» para producir la inmediata puesta a disposición judicial de toda persona detenida ilegalmente. Asimismo, por ley se determinará el plazo máximo de duración de la prisión provisional.

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Artículo 19.

Los españoles tienen derecho a elegir libremente su residencia y a circular por el territorio nacional.
Asimismo, tienen derecho a entrar y salir libremente de España en los términos que la ley establezca. Este derecho no podrá ser limitado por motivos políticos o ideológicos.

Artículo 20.

1. Se reconocen y protegen los derechos:

a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
b) A la producción y creación literaria, artística, científica y técnica.
c) A la libertad de cátedra.
d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades.

2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa.
3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España.
4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.
5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

Artículo 21.

1. Se reconoce el derecho de reunión pacífica y sin armas. El ejercicio de este derecho no necesitará autorización previa.
2. En los casos de reuniones en lugares de tránsito público y manifestaciones se dará comunicación previa a la autoridad, que sólo podrá prohibirlas cuando existan razones fundadas de alteración del orden público, con peligro para personas o bienes.

Artículo 22.

1. Se reconoce el derecho de asociación.
2. Las asociaciones que persigan fines o utilicen medios tipificados como delito son ilegales.
3. Las asociaciones constituidas al amparo de este artículo deberán inscribirse en un registro a los solos efectos de publicidad.
4. Las asociaciones sólo podrán ser disueltas o suspendidas en sus actividades en virtud de resolución judicial motivada.
5. Se prohíben las asociaciones secretas y las de carácter paramilitar.

Artículo 23.

1. Los ciudadanos tienen el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal.

2. Asimismo, tienen derecho a acceder en condiciones de igualdad a las funciones y cargos públicos, con los requisitos que señalen las leyes.

Artículo 24.

1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos.

Artículo 25.

1. Nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de producirse no constituyan delito, falta o infracción administrativa, según la legislación vigente en aquel momento.

2. Las penas privativas de libertad y las medidas de seguridad estarán orientadas hacia la reeducación y reinserción social y no podrán consistir en trabajos forzados. El condenado a pena de prisión que estuviere cumpliendo la misma gozará de los derechos fundamentales de este Capítulo, a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria. En todo caso, tendrá derecho a un trabajo remunerado y a los beneficios correspondientes de la Seguridad Social, así como al acceso a la cultura y al desarrollo integral de su personalidad.

3. La Administración civil no podrá imponer sanciones que, directa o subsidiariamente, impliquen privación de libertad.

Artículo 26.

Se prohíben los Tribunales de Honor en el ámbito de la Administración civil y de las organizaciones profesionales.

Artículo 27.

1. Todos tienen el derecho a la educación. Se reconoce la libertad de enseñanza.

2. La educación tendrá por objeto el pleno desarrollo de la personalidad humana en el respeto a los principios democráticos de convivencia y a los derechos y libertades fundamentales.

3. Los poderes públicos garantizan el derecho que asiste a los padres para que sus hijos reciban la formación religiosa y moral que esté de acuerdo con sus propias convicciones.

4. La enseñanza básica es obligatoria y gratuita.

5. Los poderes públicos garantizan el derecho de todos a la educación, mediante una programación general de la enseñanza, con participación efectiva de todos los sectores afectados y la creación de centros docentes.

6. Se reconoce a las personas físicas y jurídicas la libertad de creación de centros docentes, dentro del respeto a los principios constitucionales.

7. Los profesores, los padres y, en su caso, los alumnos intervendrán en el control y gestión de todos los centros sostenidos por la Administración con fondos públicos, en los términos que la ley establezca.

8. Los poderes públicos inspeccionarán y homologarán el sistema educativo para garantizar el cumplimiento de las leyes.

9. Los poderes públicos ayudarán a los centros docentes que reúnan los requisitos que la ley establezca.

10. Se reconoce la autonomía de las Universidades, en los términos que la ley establezca.

Artículo 28.

1. Todos tienen derecho a sindicarse libremente. La ley podrá limitar o exceptuar el ejercicio de este derecho a las Fuerzas o Institutos armados o a los demás Cuerpos sometidos a disciplina militar y regulará las peculiaridades de su ejercicio para los funcionarios públicos. La libertad sindical comprende el derecho a fundar sindicatos y a afiliarse al de su elección, así como el derecho de los sindicatos a formar confederaciones y a fundar organizaciones sindicales internacionales o a afiliarse a las mismas. Nadie podrá ser obligado a afiliarse a un sindicato.

2. Se reconoce el derecho a la huelga de los trabajadores para la defensa de sus intereses. La ley que regule el ejercicio de este derecho establecerá las garantías precisas para asegurar el mantenimiento de los servicios esenciales de la comunidad.

Artículo 29.

1. Todos los españoles tendrán el derecho de petición individual y colectiva, por escrito, en la forma y con los efectos que determine la ley.

2. Los miembros de las Fuerzas o Institutos armados o de los Cuerpos sometidos a disciplina militar podrán ejercer este derecho sólo individualmente y con arreglo a lo dispuesto en su legislación específica.

Sección 2.ª De los derechos y deberes de los ciudadanos

Artículo 30.

1. Los españoles tienen el derecho y el deber de defender a España.

2. La ley fijará las obligaciones militares de los españoles y regulará, con las debidas garantías, la objeción de conciencia, así como las demás causas de exención del servicio militar obligatorio, pudiendo imponer, en su caso, una prestación social sustitutoria.

3. Podrá establecerse un servicio civil para el cumplimiento de fines de interés general.

4. Mediante ley podrán regularse los deberes de los ciudadanos en los casos de grave riesgo, catástrofe o calamidad pública.

Artículo 31.

1. Todos contribuirán al sostenimiento de los gastos públicos de acuerdo con su capacidad económica mediante un sistema tributario justo inspirado en los principios de igualdad y progresividad que, en ningún caso, tendrá alcance confiscatorio.

2. El gasto público realizará una asignación equitativa de los recursos públicos, y su programación y ejecución responderán a los criterios de eficiencia y economía.

3. Sólo podrán establecerse prestaciones personales o patrimoniales de carácter público con arreglo a la ley.

Artículo 32.

1. El hombre y la mujer tienen derecho a contraer matrimonio con plena igualdad jurídica.

2. La ley regulará las formas de matrimonio, la edad y capacidad para contraerlo, los derechos y deberes de los cónyuges, las causas de separación y disolución y sus efectos.

Artículo 33.

1. Se reconoce el derecho a la propiedad privada y a la herencia.

2. La función social de estos derechos delimitará su contenido, de acuerdo con las leyes.

3. Nadie podrá ser privado de sus bienes y derechos sino por causa justificada de utilidad pública o interés social, mediante la correspondiente indemnización y de conformidad con lo dispuesto por las leyes.

Artículo 34.

1. Se reconoce el derecho de fundación para fines de interés general, con arreglo a la ley.
2. Regirá también para las fundaciones lo dispuesto en los apartados 2 y 4 del artículo 22.

Artículo 35.

1. Todos los españoles tienen el deber de trabajar y el derecho al trabajo, a la libre elección de profesión u oficio, a la promoción a través del trabajo y a una remuneración suficiente para satisfacer sus necesidades y las de su familia, sin que en ningún caso pueda hacerse discriminación por razón de sexo.
2. La ley regulará un estatuto de los trabajadores.

Artículo 36.

La ley regulará las peculiaridades propias del régimen jurídico de los Colegios Profesionales y el ejercicio de las profesiones tituladas. La estructura interna y el funcionamiento de los Colegios deberán ser democráticos.

Artículo 37.

1. La ley garantizará el derecho a la negociación colectiva laboral entre los representantes de los trabajadores y empresarios, así como la fuerza vinculante de los convenios.
2. Se reconoce el derecho de los trabajadores y empresarios a adoptar medidas de conflicto colectivo. La ley que regule el ejercicio de este derecho, sin perjuicio de las limitaciones que puedan establecer, incluirá las garantías precisas para asegurar el funcionamiento de los servicios esenciales de la comunidad.

Artículo 38.

Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación.

CAPÍTULO TERCERO

De los principios rectores de la política social y económica

Artículo 39.

1. Los poderes públicos aseguran la protección social, económica y jurídica de la familia.
2. Los poderes públicos aseguran, asimismo, la protección integral de los hijos, iguales éstos ante la ley con independencia de su filiación, y de las madres, cualquiera que sea su estado civil. La ley posibilitará la investigación de la paternidad.
3. Los padres deben prestar asistencia de todo orden a los hijos habidos dentro o fuera del matrimonio, durante su minoría de edad y en los demás casos en que legalmente proceda.
4. Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos.

Artículo 40.

1. Los poderes públicos promoverán las condiciones favorables para el progreso social y económico y para una distribución de la renta regional y personal más equitativa, en el marco de una política de estabilidad económica. De manera especial realizarán una política orientada al pleno empleo.
2. Asimismo, los poderes públicos fomentarán una política que garantice la formación y readaptación profesionales; velarán por la seguridad e higiene en el trabajo y garantizarán el

descanso necesario, mediante la limitación de la jornada laboral, las vacaciones periódicas retribuidas y la promoción de centros adecuados.

Artículo 41.

Los poderes públicos mantendrán un régimen público de Seguridad Social para todos los ciudadanos, que garantice la asistencia y prestaciones sociales suficientes ante situaciones de necesidad, especialmente en caso de desempleo. La asistencia y prestaciones complementarias serán libres.

Artículo 42.

El Estado velará especialmente por la salvaguardia de los derechos económicos y sociales de los trabajadores españoles en el extranjero y orientará su política hacia su retorno.

Artículo 43.

1. Se reconoce el derecho a la protección de la salud.
2. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios. La ley establecerá los derechos y deberes de todos al respecto.
3. Los poderes públicos fomentarán la educación sanitaria, la educación física y el deporte. Asimismo facilitarán la adecuada utilización del ocio.

Artículo 44.

1. Los poderes públicos promoverán y tutelarán el acceso a la cultura, a la que todos tienen derecho.
2. Los poderes públicos promoverán la ciencia y la investigación científica y técnica en beneficio del interés general.

Artículo 45.

1. Todos tienen el derecho a disfrutar de un medio ambiente adecuado para el desarrollo de la persona, así como el deber de conservarlo.
2. Los poderes públicos velarán por la utilización racional de todos los recursos naturales, con el fin de proteger y mejorar la calidad de la vida y defender y restaurar el medio ambiente, apoyándose en la indispensable solidaridad colectiva.
3. Para quienes violen lo dispuesto en el apartado anterior, en los términos que la ley fije se establecerán sanciones penales o, en su caso, administrativas, así como la obligación de reparar el daño causado.

Artículo 46.

Los poderes públicos garantizarán la conservación y promoverán el enriquecimiento del patrimonio histórico, cultural y artístico de los pueblos de España y de los bienes que lo integran, cualquiera que sea su régimen jurídico y su titularidad. La ley penal sancionará los atentados contra este patrimonio.

Artículo 47.

Todos los españoles tienen derecho a disfrutar de una vivienda digna y adecuada. Los poderes públicos promoverán las condiciones necesarias y establecerán las normas pertinentes para hacer efectivo este derecho, regulando la utilización del suelo de acuerdo con el interés general para impedir la especulación. La comunidad participará en las plusvalías que genere la acción urbanística de los entes públicos.

Artículo 48.

Los poderes públicos promoverán las condiciones para la participación libre y eficaz de la juventud en el desarrollo político, social, económico y cultural.

Artículo 49.

Los poderes públicos realizarán una política de previsión, tratamiento, rehabilitación e integración de los disminuidos físicos, sensoriales y psíquicos a los que prestarán la atención especializada que requieran y los ampararán especialmente para el disfrute de los derechos que este Título otorga a todos los ciudadanos.

Artículo 50.

Los poderes públicos garantizarán, mediante pensiones adecuadas y periódicamente actualizadas, la suficiencia económica a los ciudadanos durante la tercera edad. Asimismo, y con independencia de las obligaciones familiares, promoverán su bienestar mediante un sistema de servicios sociales que atenderán sus problemas específicos de salud, vivienda, cultura y ocio.

Artículo 51.

1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos.
2. Los poderes públicos promoverán la información y la educación de los consumidores y usuarios, fomentarán sus organizaciones y oirán a éstas en las cuestiones que puedan afectar a aquéllos, en los términos que la ley establezca.
3. En el marco de lo dispuesto por los apartados anteriores, la ley regulará el comercio interior y el régimen de autorización de productos comerciales.

Artículo 52.

La ley regulará las organizaciones profesionales que contribuyan a la defensa de los intereses económicos que les sean propios. Su estructura interna y funcionamiento deberán ser democráticos.

CAPÍTULO CUARTO

De las garantías de las libertades y derechos fundamentales

Artículo 53.

1. Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a).
2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.
3. El reconocimiento, el respeto y la protección de los principios reconocidos en el Capítulo tercero informarán la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las leyes que los desarrollen.

Artículo 54.

Una ley orgánica regulará la institución del Defensor del Pueblo, como alto comisionado de las Cortes Generales, designado por éstas para la defensa de los derechos comprendidos en este Título, a cuyo efecto podrá supervisar la actividad de la Administración, dando cuenta a las Cortes Generales.

CAPÍTULO QUINTO

De la suspensión de los derechos y libertades

Artículo 55.

1. Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción.

2. Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas.

La utilización injustificada o abusiva de las facultades reconocidas en dicha ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las leyes.

TÍTULO II

De la Corona

Artículo 56.

1. El Rey es el Jefe del Estado, símbolo de su unidad y permanencia, arbitra y modera el funcionamiento regular de las instituciones, asume la más alta representación del Estado español en las relaciones internacionales, especialmente con las naciones de su comunidad histórica, y ejerce las funciones que le atribuyen expresamente la Constitución y las leyes.

2. Su título es el de Rey de España y podrá utilizar los demás que correspondan a la Corona.

3. La persona del Rey es inviolable y no está sujeta a responsabilidad. Sus actos estarán siempre refrendados en la forma establecida en el artículo 64, careciendo de validez sin dicho refrendo, salvo lo dispuesto en el artículo 65, 2.

Artículo 57.

1. La Corona de España es hereditaria en los sucesores de S. M. Don Juan Carlos I de Borbón, legítimo heredero de la dinastía histórica. La sucesión en el trono seguirá el orden regular de primogenitura y representación, siendo preferida siempre la línea anterior a las posteriores; en la misma línea, el grado más próximo al más remoto; en el mismo grado, el varón a la mujer, y en el mismo sexo, la persona de más edad a la de menos.

2. El Príncipe heredero, desde su nacimiento o desde que se produzca el hecho que origine el llamamiento, tendrá la dignidad de Príncipe de Asturias y los demás títulos vinculados tradicionalmente al sucesor de la Corona de España.

3. Extinguidas todas las líneas llamadas en Derecho, las Cortes Generales proveerán a la sucesión en la Corona en la forma que más convenga a los intereses de España.

4. Aquellas personas que teniendo derecho a la sucesión en el trono contrajeren matrimonio contra la expresa prohibición del Rey y de las Cortes Generales, quedarán excluidas en la sucesión a la Corona por sí y sus descendientes.

5. Las abdicaciones y renuncias y cualquier duda de hecho o de derecho que ocurra en el orden de sucesión a la Corona se resolverán por una ley orgánica.

Artículo 58.

La Reina consorte o el consorte de la Reina no podrán asumir funciones constitucionales, salvo lo dispuesto para la Regencia.

Artículo 59.

1. Cuando el Rey fuere menor de edad, el padre o la madre del Rey y, en su defecto, el pariente mayor de edad más próximo a suceder en la Corona, según el orden establecido en la Constitución, entrará a ejercer inmediatamente la Regencia y la ejercerá durante el tiempo de la minoría de edad del Rey.

2. Si el Rey se inhabilitare para el ejercicio de su autoridad y la imposibilidad fuere reconocida por las Cortes Generales, entrará a ejercer inmediatamente la Regencia el Príncipe heredero de la Corona, si fuere mayor de edad. Si no lo fuere, se procederá de la manera prevista en el apartado anterior, hasta que el Príncipe heredero alcance la mayoría de edad.

3. Si no hubiere ninguna persona a quien corresponda la Regencia, ésta será nombrada por las Cortes Generales, y se compondrá de una, tres o cinco personas.

4. Para ejercer la Regencia es preciso ser español y mayor de edad.

5. La Regencia se ejercerá por mandato constitucional y siempre en nombre del Rey.

Artículo 60.

1. Será tutor del Rey menor la persona que en su testamento hubiese nombrado el Rey difunto, siempre que sea mayor de edad y español de nacimiento; si no lo hubiese nombrado, será tutor el padre o la madre mientras permanezcan viudos. En su defecto, lo nombrarán las Cortes Generales, pero no podrán acumularse los cargos de Regente y de tutor sino en el padre, madre o ascendientes directos del Rey.

2. El ejercicio de la tutela es también incompatible con el de todo cargo o representación política.

Artículo 61.

1. El Rey, al ser proclamado ante las Cortes Generales, prestará juramento de desempeñar fielmente sus funciones, guardar y hacer guardar la Constitución y las leyes y respetar los derechos de los ciudadanos y de las Comunidades Autónomas.

2. El Príncipe heredero, al alcanzar la mayoría de edad, y el Regente o Regentes al hacerse cargo de sus funciones, prestarán el mismo juramento, así como el de fidelidad al Rey.

Artículo 62.

Corresponde al Rey:

a) Sancionar y promulgar las leyes.

b) Convocar y disolver las Cortes Generales y convocar elecciones en los términos previstos en la Constitución.

c) Convocar a referéndum en los casos previstos en la Constitución.

d) Proponer el candidato a Presidente del Gobierno y, en su caso, nombrarlo, así como poner fin a sus funciones en los términos previstos en la Constitución.

e) Nombrar y separar a los miembros del Gobierno, a propuesta de su Presidente.

f) Expedir los decretos acordados en el Consejo de Ministros, conferir los empleos civiles y militares y conceder honores y distinciones con arreglo a las leyes.

g) Ser informado de los asuntos de Estado y presidir, a estos efectos, las sesiones del Consejo de Ministros, cuando lo estime oportuno, a petición del Presidente del Gobierno.

h) El mando supremo de las Fuerzas Armadas.

i) Ejercer el derecho de gracia con arreglo a la ley, que no podrá autorizar indultos generales.

j) El Alto Patronazgo de las Reales Academias.

Artículo 63.

1. El Rey acredita a los embajadores y otros representantes diplomáticos. Los representantes extranjeros en España están acreditados ante él.

2. Al Rey corresponde manifestar el consentimiento del Estado para obligarse internacionalmente por medio de tratados, de conformidad con la Constitución y las leyes.

3. Al Rey corresponde, previa autorización de las Cortes Generales, declarar la guerra y hacer la paz.

Artículo 64.

1. Los actos del Rey serán refrendados por el Presidente del Gobierno y, en su caso, por los Ministros competentes. La propuesta y el nombramiento del Presidente del Gobierno, y la disolución prevista en el artículo 99, serán refrendados por el Presidente del Congreso.
2. De los actos del Rey serán responsables las personas que los refrenden.

Artículo 65.

1. El Rey recibe de los Presupuestos del Estado una cantidad global para el sostenimiento de su Familia y Casa, y distribuye libremente la misma.
2. El Rey nombra y releva libremente a los miembros civiles y militares de su Casa.

[. . .]

§ 3

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Última modificación: 27 de mayo de 2021
Referencia: BOE-A-2018-16673

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus

orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también

riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra

sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de

todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de

discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones

tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la ley.*

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.*

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Artículo 3. *Datos de las personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4. *Exactitud de los datos.*

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5. *Deber de confidencialidad.*

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 6. *Tratamiento basado en el consentimiento del afectado.*

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 7. *Consentimiento de los menores de edad.*

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 9. *Categorías especiales de datos.*

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10. *Tratamiento de datos de naturaleza penal.*

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I

Transparencia e información

Artículo 11. *Transparencia e información al afectado.*

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

CAPÍTULO II

Ejercicio de los derechos

Artículo 12. *Disposiciones generales sobre ejercicio de los derechos.*

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. *Derecho de acceso.*

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales

que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. *Derecho de rectificación.*

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15. *Derecho de supresión.*

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. *Derecho a la limitación del tratamiento.*

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. *Derecho a la portabilidad.*

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18. *Derecho de oposición.*

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

Artículo 19. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Artículo 20. *Sistemas de información crediticia.*

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21. *Tratamientos relacionados con la realización de determinadas operaciones mercantiles.*

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22. *Tratamientos con fines de videovigilancia.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá

por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23. *Sistemas de exclusión publicitaria.*

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Artículo 24. *Sistemas de información de denuncias internas.*

1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

5. Los principios de los apartados anteriores serán aplicables a los sistemas de denuncias internas que pudieran crearse en las Administraciones Públicas.

Artículo 25. *Tratamiento de datos en el ámbito de la función estadística pública.*

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26. *Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.*

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27. *Tratamiento de datos relativos a infracciones y sanciones administrativas.*

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28. *Obligaciones generales del responsable y encargado del tratamiento.*

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.*

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

Artículo 31. *Registro de las actividades de tratamiento.*

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Artículo 32. *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste

evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Encargado del tratamiento

Artículo 33. *Encargado del tratamiento.*

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III

Delegado de protección de datos

Artículo 34. *Designación de un delegado de protección de datos.*

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. *Cualificación del delegado de protección de datos.*

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación

universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. *Posición del delegado de protección de datos.*

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. *Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.*

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV

Códigos de conducta y certificación

Artículo 38. *Códigos de conducta.*

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de

empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39. *Acreditación de instituciones de certificación.*

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40. *Régimen de las transferencias internacionales de datos.*

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. *Supuestos de adopción por la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42. *Supuestos sometidos a autorización previa de las autoridades de protección de datos.*

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43. *Supuestos sometidos a información previa a la autoridad de protección de datos competente.*

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I

La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44. *Disposiciones generales.*

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 45. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46. *Régimen económico presupuestario y de personal.*

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47. *Funciones y potestades de la Agencia Española de Protección de Datos.*

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el Título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,
b) incapacidad sobrevenida para el ejercicio de su función,
c) incompatibilidad, o
d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Artículo 49. *Consejo Consultivo de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un Diputado, propuesto por el Congreso de los Diputados.
b) Un Senador, propuesto por el Senado.
c) Un representante designado por el Consejo General del Poder Judicial.
d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.
e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.
f) Un experto propuesto por la Federación Española de Municipios y Provincias.
g) Un experto propuesto por el Consejo de Consumidores y Usuarios.
h) Dos expertos propuestos por las Organizaciones Empresariales.
i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.
j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.
k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.

l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.

m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.

n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.

ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50. *Publicidad.*

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Sección 2.ª Potestades de investigación y planes de auditoría preventiva

Artículo 51. *Ámbito y personal competente.*

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 52. *Deber de colaboración.*

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 54. *Planes de auditoría.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55. *Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56. *Acción exterior.*

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II

Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57. *Autoridades autonómicas de protección de datos.*

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58. *Cooperación institucional.*

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente

la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59. *Tratamientos contrarios al Reglamento (UE) 2016/679.*

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60. *Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.*

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61. *Intervención en caso de tratamientos transfronterizos.*

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62. *Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.*

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63. *Régimen jurídico.*

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64. *Forma de iniciación del procedimiento y duración.*

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 75 de esta ley orgánica.

Admitida a trámite la reclamación así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679. Será en este caso de aplicación lo dispuesto en el apartado 1 y en los párrafos primero, tercero, cuarto y quinto del apartado 2.

4. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo

de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

Artículo 65. *Admisión a trámite de las reclamaciones.*

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento o al organismo de supervisión establecido para la aplicación de los códigos de conducta a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este Título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos.

Artículo 66. *Determinación del alcance territorial.*

1. Salvo en los supuestos a los que se refiere el artículo 64.3 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 67. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la Sección 2.ª del Capítulo I del Título VII de esta ley orgánica y no podrán tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica.

Artículo 68. *Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69. *Medidas provisionales y de garantía de los derechos.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70. *Sujetos responsables.*

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71. *Infracciones.*

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72. *Infracciones consideradas muy graves.*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.
c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.
d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.
e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.
f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.
g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.
h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.
i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.
j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.
k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías,

requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73. *Infracciones consideradas graves.*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera

producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74. *Infracciones consideradas leves.*

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75. *Interrupción de la prescripción de la infracción.*

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas.

Artículo 76. *Sanciones y medidas correctivas.*

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.

4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.

Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.*

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Artículo 78. *Prescripción de las sanciones.*

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.
b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.
c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.
3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79. *Los derechos en la Era digital.*

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. *Derecho a la neutralidad de Internet.*

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81. *Derecho de acceso universal a Internet.*

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.
2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.
3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.
4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.
5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.
6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. *Derecho a la seguridad digital.*

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83. *Derecho a la educación digital.*

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y

la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. *Protección de los menores en Internet.*

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.*

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.*

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados

anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. *Derechos digitales en la negociación colectiva.*

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. *Protección de datos de los menores en Internet.*

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios

de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.*

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96. *Derecho al testamento digital.*

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. *Políticas de impulso de los derechos digitales.*

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. *Medidas de seguridad en el ámbito del sector público.*

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. *Protección de datos y transparencia y acceso a la información pública.*

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. *Cómputo de plazos.*

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. *Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.*

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. *Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.*

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. *Incorporación de deudas a sistemas de información crediticia.*

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. *Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.*

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo

cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Disposición adicional octava. *Potestad de verificación de las Administraciones Públicas.*

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Disposición adicional novena. *Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.*

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Disposición adicional décima. *Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.*

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Disposición adicional undécima. *Privacidad en las comunicaciones electrónicas.*

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. *Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.*

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. *Transferencias internacionales de datos tributarios.*

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. *Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.*

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

Disposición adicional decimosexta. *Prácticas agresivas en materia de protección de datos.*

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica

de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. *Tratamientos de datos de salud.*

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de

actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. *Criterios de seguridad.*

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. *Derechos de los menores ante Internet.*

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. *Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.*

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. *Educación digital.*

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. *Acceso a los archivos públicos y eclesiásticos.*

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición transitoria primera. *Estatuto de la Agencia Española de Protección de Datos.*

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.
2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. *Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. *Régimen transitorio de los procedimientos.*

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. *Tratamientos sometidos a la Directiva (UE) 2016/680.*

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

> Téngase en cuenta que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido transpuesta por la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806

Disposición transitoria quinta. *Contratos de encargado del tratamiento.*

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. *Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.*

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. *Derogación normativa.*

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. *Naturaleza de la presente ley.*

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

– El Título IV,
– el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,
– el Título VIII,
– el Título IX,
– los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,
– las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,
– las disposiciones transitorias,
– y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. *Título competencial.*

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.ª y 18.ª de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.ª de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.ª de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.ª de la Constitución.

Disposición final tercera. *Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.*

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:

Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

> «3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas

las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

«Artículo cincuenta y ocho bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales.*

1. **(Anulado)**
2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.
3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.
4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.
5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

Disposición final cuarta. *Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. […]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[…]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por

parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.*

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. *Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.*

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. *Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá

acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«Artículo 15 bis. *Intervención en procesos de defensa de la competencia y de protección de datos.*

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del

importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. *Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.*

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. *Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«Artículo 16. *[…]*

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. *Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.*

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

> «l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

> **«Artículo 6 bis.** *Registro de actividades de tratamiento.*
>
> Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

Dos. El apartado 1 del artículo 15 queda redactado como sigue:

> «1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.
>
> Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Disposición final duodécima. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

> **«Artículo 28.** *[…]*
>
> 2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.
>
> Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.
>
> Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará

al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. *Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.*

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

«Artículo 20 bis. *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. *Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.*

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

«j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimoquinta. *Desarrollo normativo.*

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. *Entrada en vigor.*

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 4

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Última modificación: 8 de marzo de 2012
Referencia: BOE-A-2008-979

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.*

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. *Plazos de implantación de las medidas de seguridad.*

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. *Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.*

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. *Régimen transitorio de los procedimientos.*

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. *Régimen transitorio de las actuaciones previas.*

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del

tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. *Título competencial.*

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Ámbito objetivo de aplicación.*

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. *Ámbito territorial de aplicación.*

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. *Ficheros o tratamientos excluidos.*

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. *Definiciones.*

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. *Cómputo de plazos.*

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. *Fuentes accesibles al público.*

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

TÍTULO II

Principios de protección de datos

CAPÍTULO I

Calidad de los datos

Artículo 8. *Principios relativos a la calidad de los datos.*

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. *Tratamiento con fines estadísticos, históricos o científicos.*

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. *Supuestos que legitiman el tratamiento o cesión de los datos.*

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) **(Anulado)**

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. *Verificación de datos en solicitudes formuladas a las Administraciones públicas.*

(Anulado)

CAPÍTULO II

Consentimiento para el tratamiento de los datos y deber de información

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. *Principios generales.*

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. *Forma de recabar el consentimiento.*

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. *Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.*

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. *Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.*

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. *Revocación del consentimiento.*

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección 2.ª Deber de información al interesado

Artículo 18. *Acreditación del cumplimiento del deber de información.*

(Anulado)

Artículo 19. *Supuestos especiales.*

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Encargado del tratamiento

Artículo 20. *Relaciones entre el responsable y el encargado del tratamiento.*

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. *Posibilidad de subcontratación de los servicios.*

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. *Conservación de los datos por el encargado del tratamiento.*

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III

Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I

Disposiciones generales

Artículo 23. *Carácter personalísimo.*

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. *Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. *Procedimiento.*

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. *Ejercicio de los derechos ante un encargado del tratamiento.*

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

CAPÍTULO II

Derecho de acceso

Artículo 27. *Derecho de acceso.*

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. *Ejercicio del derecho de acceso.*

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.
c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.
3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.
Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. *Otorgamiento del acceso.*

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.
En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.
2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.
3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. *Denegación del acceso.*

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.
2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Derechos de rectificación y cancelación

Artículo 31. *Derechos de rectificación y cancelación.*

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. *Ejercicio de los derechos de rectificación y cancelación.*

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. *Denegación de los derechos de rectificación y cancelación.*

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV

Derecho de oposición

Artículo 34. *Derecho de oposición.*

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. *Ejercicio del derecho de oposición.*

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. *Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.*

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV

Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª Disposiciones generales

Artículo 37. *Régimen aplicable.*

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se

someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. *Requisitos para la inclusión de los datos.*

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada **y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.**

> Téngase en cuenta que se anula el inciso destacado de la letra a) del apartado 1 por Sentencias del TS de 15 de julio de 2010. Ref. BOE-A-2010-16299 y Ref. BOE-A-2010-16301

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. **(Anulado)**

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. *Información previa a la inclusión.*

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán

ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. *Notificación de inclusión.*

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. *Conservación de los datos.*

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. *Acceso a la información contenida en el fichero.*

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.

b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.

c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. *Responsabilidad.*

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. *Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. *Datos susceptibles de tratamiento e información al interesado.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este

reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. *Tratamiento de datos en campañas publicitarias.*

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. *Depuración de datos personales.*

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. *Ficheros de exclusión del envío de comunicaciones comerciales.*

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. *Ficheros comunes de exclusión del envío de comunicaciones comerciales.*

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para

evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. *Derechos de acceso, rectificación y cancelación.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. *Derecho de oposición.*

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V

Obligaciones previas al tratamiento de los datos

CAPÍTULO I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. *Disposición o Acuerdo de creación, modificación o supresión del fichero.*

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. *Forma de la disposición o acuerdo.*

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. *Contenido de la disposición o acuerdo.*

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. *Notificación de ficheros.*

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. *Tratamiento de datos en distintos soportes.*

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. *Ficheros en los que exista más de un responsable.*

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. *Notificación de la modificación o supresión de ficheros.*

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. *Modelos y soportes para la notificación.*

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. *Inscripción de los ficheros.*

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. *Cancelación de la inscripción.*

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. *Rectificación de errores.*

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. *Inscripción de oficio de ficheros de titularidad pública.*

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. *Colaboración con las autoridades de control de las comunidades autónomas.*

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.*

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. *Autorización y notificación.*

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. *Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.*

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. *Nivel adecuado de protección declarado por Decisión de la Comisión Europea.*

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. *Suspensión temporal de las transferencias.*

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. *Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.*

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de

diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII

Códigos tipo

Artículo 71. *Objeto y naturaleza.*

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. *Iniciativa y ámbito de aplicación.*

1. Los códigos tipo tendrán carácter voluntario.
2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.
3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.
4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. *Contenido.*

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.
2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
b) Las previsiones específicas para la aplicación de los principios de protección de datos.
c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:
a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.
b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.
c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. *Compromisos adicionales.*

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.
2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.
b) La identificación de las categorías de cesionarios o importadores de los datos.
c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.
d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. *Garantías del cumplimiento de los códigos tipo.*

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.

b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

c) El principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. *Relación de adheridos.*

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. *Depósito y publicidad de los códigos tipo.*

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. *Obligaciones posteriores a la inscripción del código tipo.*

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. *Alcance.*

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. *Niveles de seguridad.*

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. *Aplicación de los niveles de seguridad.*

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.
5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.
8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. *Encargado del tratamiento.*

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.
3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. *Prestaciones de servicios sin acceso a datos personales.*

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos

del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. *Delegación de autorizaciones.*

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. *Acceso a datos a través de redes de comunicaciones.*

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. *Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. *Ficheros temporales o copias de trabajo de documentos.*

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. *Control de acceso.*

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. *Gestión de soportes y documentos.*

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. *Identificación y autenticación.*

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. *Copias de respaldo y recuperación.*

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. *Responsable de seguridad.*

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. *Auditoría.*

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. *Gestión de soportes y documentos.*

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. *Identificación y autenticación.*

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. *Registro de incidencias.*

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. *Gestión y distribución de soportes.*

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. *Copias de respaldo y recuperación.*

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos

informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. *Registro de accesos.*

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. *Telecomunicaciones.*

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. *Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.

b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. *Criterios de archivo.*

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. *Dispositivos de almacenamiento.*

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. *Custodia de los soportes.*

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. *Responsable de seguridad.*

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. *Auditoría.*

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. *Almacenamiento de la información.*

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. *Copia o reproducción.*

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. *Acceso a la documentación.*

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. *Traslado de documentación.*

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO IX

Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I

Disposiciones generales

Artículo 115. *Régimen aplicable.*

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. *Publicidad de las resoluciones.*

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.
2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.
3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. *Instrucción del procedimiento.*

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. *Ejecución de la resolución.*

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección 1.ª Disposiciones generales

Artículo 120. *Ámbito de aplicación.*

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el ar-tículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. *Inmovilización de ficheros.*

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección 2.ª Actuaciones previas

Artículo 122. *Iniciación.*

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. *Personal competente para la realización de las actuaciones previas.*

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. **(Anulado)**

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. *Obtención de información.*

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. *Actuaciones presenciales.*

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. *Resultado de las actuaciones previas.*

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección 3.ª Procedimiento sancionador

Artículo 127. *Iniciación del procedimiento.*

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.

b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.

d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. *Plazo máximo para resolver.*

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.

2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. *Disposición general.*

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. *Iniciación del procedimiento.*

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.

2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. *Especialidades en la notificación de ficheros de titularidad pública.*

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el ar-tículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. *Acuerdo de inscripción o cancelación.*

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. *Improcedencia o denegación de la inscripción.*

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos

Artículo 135. *Iniciación del procedimiento.*

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. *Terminación del expediente.*

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.
Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. *Iniciación del procedimiento.*

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.
2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.
b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.
Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. *Instrucción del procedimiento.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un

período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. *Actos posteriores a la resolución.*

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. *Iniciación.*

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. *Instrucción y resolución.*

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. *Actos posteriores a la resolución.*

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. *Levantamiento de la suspensión temporal.*

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI

Procedimiento de inscripción de códigos tipo

Artículo 145. *Iniciación del procedimiento.*

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.

b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.

c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.

f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. *Análisis de los aspectos sustantivos del código tipo.*

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. *Información pública.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. *Mejora del código tipo.*

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. *Trámite de audiencia.*

En caso de que durante el trámite previsto en el ar-tículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. *Resolución.*

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.

2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. *Publicación de los códigos tipo por la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección 1.ª Procedimiento de exención del deber de información al interesado

Artículo 153. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.

2. En el escrito de solicitud, además de los requisitos recogidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.

b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.

c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.

d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. *Propuesta de nuevas medidas compensatorias.*

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. *Terminación del procedimiento.*

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.

b) Motivar expresamente las causas que justificarían la declaración.

c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. *Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. *Aplicación supletoria.*

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.

§ 5

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Unión Europea
«DOUE» núm. 119, de 4 de mayo de 2016
Última modificación: sin modificaciones
Referencia: DOUE-L-2016-89807

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo [1],

Visto el dictamen del Comité de las Regiones [2],

De conformidad con el procedimiento legislativo ordinario [3],

Considerando lo siguiente:

(1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

(3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo [4] trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

(4) El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe

considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(7) Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(8) En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento.

(9) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE.

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión

realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

(12) El artículo 16, apartado 2, del TFUE encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos.

(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión [(5)].

(14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

(15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con

actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(17) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo [(6)] se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(19) La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo [(7)]. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

(20) Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados

miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

(21) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo [(8)], en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

(22) Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

(23) Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que se encuentran en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que se encuentran en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

(24) El tratamiento de datos personales de los interesados que se encuentran en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente Reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

(25) Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro.

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de

información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

(27) El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

(31) Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las

actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

(34) Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

(35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo [(9)]; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

(36) El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

(37) Un grupo empresarial debe estar constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

(38) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

(41) Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

(42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración

por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo [10], debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

(44) El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

(45) Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo,

cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

(48) Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

(49) Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para

lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo [(11)], es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

(55) Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

(57) Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

(58) El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le

conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

(59) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

(60) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

(63) Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener

como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

(64) El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

(67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

(68) Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

(70) Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para

los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(72) La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto.

(73) El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

(77) Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(79) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

(80) El responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que se encuentran en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. El representante debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe

desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

(82) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de

sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

(89) La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

(90) En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular

gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(91) Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria.

(92) Hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.

(93) Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

(94) Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas.

(95) El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la

realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control.

(96) Deben llevarse también a cabo consultas con la autoridad de control en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de mitigar el riesgo que implique el tratamiento para el interesado.

(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

(98) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento.

(99) Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas.

(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(102) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

(105) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

(106) La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo [(12)], establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de

datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente.

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

(111) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si

estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado.

(112) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

(113) Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado.

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

(115) Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros. Esto puede incluir sentencias de órganos jurisdiccionales o decisiones de autoridades administrativas de terceros países que obliguen a un responsable o un encargado del tratamiento a transferir o comunicar datos personales, y que no se basen en un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país requirente y la Unión o un Estado miembro. La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer

los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento.

(117) El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

(118) La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

(119) Si un Estado miembro establece varias autoridades de control, debe disponer por ley mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Tal Estado miembro debe, en particular, designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control, el Comité y la Comisión.

(120) Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

(121) Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

(122) Cada autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el presente Reglamento. Lo anterior debe abarcar, en particular, el tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio de su Estado miembro, el tratamiento de datos personales realizado por autoridades públicas o por organismos privados que actúen en interés público, el tratamiento que afecte a interesados en su territorio, o el tratamiento realizado por un responsable o un encargado que no esté establecido en la Unión cuando sus destinatarios sean interesados residentes en su territorio. Debe incluirse el examen de reclamaciones

presentadas por un interesado, la realización de investigaciones sobre la aplicación del presente Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

(123) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación.

(124) Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal. Dicha autoridad debe cooperar con las demás autoridades interesadas, ya sea porque el responsable o el encargado tenga un establecimiento en el territorio de su Estado miembro, porque afecte sustancialmente a interesados que residen en su territorio, o porque se haya presentado una reclamación ante ellas. Asimismo, cuando un interesado que no resida en ese Estado miembro haya presentado una reclamación, la autoridad de control ante la que se haya presentado esta también debe ser autoridad de control interesada. En el marco de sus funciones de formulación de directrices sobre cualquier cuestión relacionada con la aplicación del presente Reglamento, el Comité debe estar facultado para formular directrices, en particular sobre los criterios que han de tenerse en cuenta para determinar si el tratamiento en cuestión afecta sustancialmente a interesados de más de un Estado miembro y sobre lo que constituya una objeción pertinente y motivada.

(125) La autoridad principal debe ser competente para adoptar decisiones vinculantes relativas a las medidas de aplicación de los poderes conferidos con arreglo al presente Reglamento. En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones. En los casos en los que la decisión consista en rechazar total o parcialmente la reclamación del interesado, esa decisión debe ser adoptada por la autoridad de control ante la que se haya presentado la reclamación.

(126) La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas y debe dirigirse al establecimiento principal o único del responsable o del encargado del tratamiento y ser vinculante para ambos. El responsable o el encargado deben tomar las medidas necesarias para garantizar el cumplimiento del presente Reglamento y la aplicación de la decisión notificada por la autoridad de control principal al establecimiento principal del responsable o del encargado en lo que se refiere a las actividades de tratamiento en la Unión.

(127) Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la

autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante la posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única.

(128) Las normas sobre la autoridad de control principal y el mecanismo de ventanilla única no deben aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente para ejercer los poderes conferidos con arreglo al presente Reglamento debe ser la autoridad de control del Estado miembro en el que estén establecidos la autoridad pública o el organismo privado.

(129) Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

(130) Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente.

(131) En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el

tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros.

(132) Entre las actividades de sensibilización del público por parte de las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas y las pequeñas y medianas empresas, así como las personas físicas, en particular en el contexto educativo.

(133) Las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior. Una autoridad de control que solicite asistencia mutua puede adoptar una medida provisional si no recibe respuesta a su solicitud de asistencia en el plazo de un mes a partir de su recepción por la otra autoridad de control.

(134) Cada autoridad de control debe participar, cuando proceda, en operaciones conjuntas con otras autoridades de control. La autoridad de control a la que se solicite ayuda debe tener la obligación de responder a la solicitud en un plazo de tiempo determinado.

(135) A fin de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia para la cooperación entre las autoridades de control. Este mecanismo debe aplicarse en particular cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados.

(136) En aplicación del mecanismo de coherencia, el Comité debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría de sus miembros o si así lo solicita cualquier autoridad de control interesada o la Comisión. El Comité también debe estar facultado para adoptar decisiones jurídicamente vinculantes en caso de diferencias entre autoridades de control. A tal efecto debe dictar, en principio por mayoría de dos tercios de sus miembros, decisiones jurídicamente vinculantes en casos claramente especificados en los que exista conflicto de opiniones entre las autoridades de control, en particular en el mecanismo de cooperación entre la autoridad de control principal y las autoridades de control interesadas sobre el fondo del asunto, especialmente en caso de infracción del presente Reglamento.

(137) La necesidad urgente de actuar puede obedecer a la necesidad de proteger los derechos y libertades de los interesados, en particular cuando exista el riesgo de que pueda verse considerablemente obstaculizado el reconocimiento de alguno de sus derechos. Por lo tanto, una autoridad de control debe poder adoptar en su territorio medidas provisionales, debidamente justificadas, con un plazo de validez determinado no superior a tres meses.

(138) La aplicación de tal mecanismo debe ser una condición para la licitud de una medida de una autoridad de control destinada a producir efectos jurídicos, en aquellos casos en los que su aplicación sea obligatoria. En otros casos de relevancia transfronteriza, la autoridad de control principal y las autoridades de control interesadas deben aplicar entre sí el mecanismo de cooperación, y las autoridades de control interesadas pueden prestarse asistencia mutua y realizar entre sí operaciones conjuntas, sobre una base bilateral o multilateral, sin tener que aplicarlo.

(139) A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de

Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones.

(140) El Comité debe contar con una secretaría, a cargo el Supervisor Europeo de Protección de Datos. El personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones conferidas al Comité por el presente Reglamento debe desempeñar sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité y responder ante él.

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(142) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

(143) Toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité, en las condiciones establecidas en el artículo 263 del TFUE. Como destinatarias de dichas decisiones, las autoridades de control interesadas que quieran impugnarlas tienen que interponer recurso en el plazo de dos meses a partir del momento en que les fueron notificadas, de conformidad con el artículo 263 del TFUE. En caso de que las decisiones del Comité afecten directa e individualmente a un responsable, un encargado o al reclamante, estos pueden interponer recurso de anulación de dichas decisiones en el plazo de dos meses a partir de su publicación en el sitio web del Comité, de conformidad con el artículo 263 del TFUE. Sin perjuicio de lo dispuesto en el artículo 263 del TFUE, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva ante el tribunal nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le afecten. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el

asesoramiento facilitado por ellas. Las acciones contra una autoridad de control deben ejercitarse ante los tribunales del Estado miembro en el que esté establecida y tramitarse con arreglo al Derecho procesal de dicho Estado miembro. Dichos tribunales deben tener plena jurisdicción, incluida la competencia para examinar todos los elementos de hecho y de Derecho relativos a la causa de la que conozcan.

Si una autoridad de control rechaza o desestima una reclamación, el reclamante puede ejercitar una acción ante los tribunales del mismo Estado miembro. En el contexto de las acciones judiciales relacionadas con la aplicación del presente Reglamento, los tribunales nacionales que estimen necesaria una decisión al respecto para poder emitir su fallo pueden, o en el caso establecido en el artículo 267 del TFUE, deben solicitar al Tribunal de Justicia que se pronuncie con carácter prejudicial sobre la interpretación del Derecho de la Unión, incluido el presente Reglamento. Además, si una decisión de una autoridad de control por la que se ejecuta una decisión del Comité se impugna ante un tribunal nacional y se cuestiona la validez de la decisión del Comité, dicho tribunal nacional no es competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tiene que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del TFUE, según la interpretación de este. No obstante, un tribunal nacional puede no remitir la cuestión de la validez de la decisión del Comité a instancia de una persona física o jurídica que, habiendo tenido la oportunidad de interponer recurso de anulación de dicha decisión, en particular si dicha decisión la afectaba directa e individualmente, no lo hizo en el plazo establecido en el artículo 263 del TFUE.

(144) Si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento, como tener el mismo asunto con respecto a un tratamiento por el mismo responsable o encargado, o la misma causa de la acción, debe ponerse en contacto con ese tribunal para confirmar la existencia de tales acciones conexas. Si dichas acciones conexas están pendientes ante un tribunal de otro Estado miembro, cualquier otro tribunal distinto de aquel ante el cual se ejercitó la acción en primer lugar puede suspender el procedimiento o, a instancia de una de las partes, inhibirse a favor del tribunal ante el cual se ejercitó la acción en primer lugar si este último es competente para su conocimiento y su acumulación es conforme a Derecho. Se consideran conexas las acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas.

(145) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre

que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

(147) En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo [13] deben entenderse sin perjuicio de la aplicación de dichas normas específicas.

(148) A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(149) Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio ne bis in idem, según la interpretación del Tribunal de Justicia.

(150) A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, la autoridad de control debe tener en cuenta al valorar la cuantía apropiada de la multa el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. El mecanismo de coherencia también puede emplearse para fomentar una aplicación coherente de las multas administrativas. Debe corresponder a los Estados miembros determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas. La imposición de una multa administrativa o de una advertencia no afecta al ejercicio de otras competencias de las autoridades de control ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(151) Los ordenamientos jurídicos de Dinamarca y Estonia no permiten las multas administrativas según lo dispuesto en el presente Reglamento. Las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por la autoridad de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto

equivalente a las multas administrativas impuestas por las autoridades de control. Por lo tanto los tribunales nacionales competentes deben tener en cuenta la recomendación de la autoridad de control que incoe la multa. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

(152) En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(153) El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

(154) El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo [(14)] no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(155) El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la

ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

(156) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

(157) Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

(158) El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe se de aplicación a personas fallecidas. Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de

manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.

(160) El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas.

(161) Al objeto de otorgar el consentimiento para la participación en actividades de investigación científica en ensayos clínicos, deben aplicarse las disposiciones pertinentes del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo [15].

(162) El presente Reglamento debe aplicarse al tratamiento de datos personales con fines estadísticos. El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas.

(163) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos fijados en el artículo 338, apartado 2, del TFUE, mientras que las estadísticas nacionales deben cumplir asimismo el Derecho de los Estados miembros. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo [16] facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(164) Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión.

(165) El presente Reglamento respeta y no prejuzga el estatuto reconocido en los Estados miembros, en virtud del Derecho constitucional, a las iglesias y las asociaciones o comunidades religiosas, tal como se reconoce en el artículo 17 del TFUE.

(166) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de conformidad con el artículo 290 del TFUE. En particular, deben adoptarse actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar

dichos iconos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

(168) El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; códigos de conducta; normas técnicas y mecanismos de certificación; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional; cláusulas tipo de protección; formatos y procedimientos para el intercambio de información entre responsables, encargados y autoridades de control respecto de normas corporativas vinculantes; asistencia mutua; y modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre las autoridades de control y el Comité.

(169) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando las pruebas disponibles muestren que un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado y así lo requieran razones imperiosas de urgencia.

(170) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(171) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

(172) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, y éste emitió su dictamen el 7 de marzo de 2012 [17].

(173) El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo [18], incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

HAN ADOPTADO EL PRESENTE REGLAMENTO

---

(1) DO C 229 de 31.7.2012, p. 90.

(2) DO C 391 de 18.12.2012, p. 127.

(3) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.

(4) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

(5) Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas [C(2003) 1422] (DO L 124 de 20.5.2003, p. 36).

(6) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(7) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (véase la página 89 del presente Diario Oficial).

(8) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

(9) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

(10) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

(11) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

(12) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(13) Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

(14) Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

(15) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

(16) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

(17) DO C 192 de 30.6.2012, p. 7.

(18) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2. *Ámbito de aplicación material.*

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.
4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3. *Ámbito territorial.*

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4. *Definiciones.*

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o

cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las

decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo [(19)];

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

[19] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

CAPÍTULO II

Principios

Artículo 5. *Principios relativos al tratamiento.*

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6. *Licitud del tratamiento.*

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7. *Condiciones para el consentimiento.*

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. *Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.*

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 9. *Tratamiento de categorías especiales de datos personales.*

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo

perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10. *Tratamiento de datos personales relativos a condenas e infracciones penales.*

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11. *Tratamiento que no requiere identificación.*

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III

Derechos del interesado

Sección 1. Transparencia y modalidades

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2. Información y acceso a los datos personales

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.*

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e) el derecho a presentar una reclamación ante una autoridad de control;
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.
5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza legal.

Artículo 15. *Derecho de acceso del interesado.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Artículo 16. *Derecho de rectificación.*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17. *Derecho de supresión («el derecho al olvido»).*

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18. *Derecho a la limitación del tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales en un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19. *Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.*

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20. *Derecho a la portabilidad de los datos.*

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21. *Derecho de oposición.*

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.
4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.
5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.
6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles.*

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Artículo 23. *Limitaciones.*

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;
f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento;
g) los riesgos para los derechos y libertades de los interesados, y
h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Artículo 24. *Responsabilidad del responsable del tratamiento.*

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.
3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25. *Protección de datos desde el diseño y por defecto.*

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26. *Corresponsables del tratamiento.*

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados

miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27. *Representantes de responsables o encargados del tratamiento no establecidos en la Unión.*

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.

2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:

a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 28. *Encargado del tratamiento.*

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30. *Registro de las actividades de tratamiento.*

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31. *Cooperación con la autoridad de control.*

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Artículo 32. *Seguridad del tratamiento.*

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control.*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36. *Consulta previa.*

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no

haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4. Delegado de protección de datos

Artículo 37. *Designación del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38. *Posición del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39. *Funciones del delegado de protección de datos.*

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Artículo 40. *Códigos de conducta.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de

tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41. *Supervisión de códigos de conducta aprobados.*

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;

b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;

c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los requisitos de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.

4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si los requisitos de acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.

6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42. *Certificación.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los criterios pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los criterios para la certificación.

8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43. *Organismo de certificación.*

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del artículo 55 o 56;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo [20] con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los requisitos aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56 o por el Comité en virtud del artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.º 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.

5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité.

7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.

9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

---

[20] Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44. *Principio general de las transferencias.*

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45. *Transferencias basadas en una decisión de adecuación.*

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las

decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46. *Transferencias mediante garantías adecuadas.*

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47. *Normas corporativas vinculantes.*

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48. *Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.*

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50. *Cooperación internacional en el ámbito de la protección de datos personales.*

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1. Independencia

Artículo 51. *Autoridad de control.*

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.

3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.

4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52. *Independencia.*

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53. *Condiciones generales aplicables a los miembros de la autoridad de control.*

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,
— su Gobierno,
— su Jefe de Estado, o
— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.
3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.
4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54. *Normas relativas al establecimiento de la autoridad de control.*

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;
b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;
c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;
d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;
e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;
f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2. Competencia, funciones y poderes

Artículo 55. *Competencia.*

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.
2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.

3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56. *Competencia de la autoridad de control principal.*

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57. *Funciones.*

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los requisitos para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58. *Poderes.*

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59. *Informe de actividad.*

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII

Cooperación y coherencia

Sección 1. Cooperación y coherencia

Artículo 60. *Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.*

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.

5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y

las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61. *Asistencia mutua.*

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas

adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.

9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62. *Operaciones conjuntas de las autoridades de control.*

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.

2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.

3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida.

4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.

5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.

6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.

7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2. Coherencia

Artículo 63. *Mecanismo de coherencia.*

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64. *Dictamen del Comité.*

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los requisitos para la acreditación de un organismo con arreglo al artículo 41, apartado 3, de un organismo de certificación conforme al artículo 43, apartado 3, o los criterios aplicables a la certificación a que se refiere el artículo 42, apartado 5;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.

3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.

4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.

5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:

a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y

b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.

6. La autoridad de control competente a que se refiere el apartado 1 no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.

7. La autoridad de control competente a que se refiere el apartado 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control competente a que se refiere el apartado 1 informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65. *Resolución de conflictos por el Comité.*

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad de control principal y esta no haya seguido la objeción o haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del

tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66. *Procedimiento de urgencia.*

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.

4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité.

Artículo 67. *Intercambio de información.*

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3. Comité europeo de protección de datos

Artículo 68. *Comité Europeo de Protección de Datos.*

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2. El Comité estará representado por su presidente.

3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas

aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69. *Independencia.*

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartados 1 y 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70. *Funciones del Comité.*

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:

a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;

b) asesorará a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento;

c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;

d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;

e) examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;

f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;

g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;

i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;

j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;

k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;

l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas;

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) aprobará los criterios de certificación en virtud del artículo 42, apartado 5, y llevará un registro público de los mecanismos de certificación y sellos y marcas de protección de datos en virtud del artículo 42, apartado 8, y de los responsables o los encargados del tratamiento certificados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) aprobará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación a los que se refiere el artículo 43;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

u) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control;

v) promoverá programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71. *Informes.*

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72. *Procedimiento.*

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.
2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73. *Presidencia.*

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.
2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74. *Funciones del presidente.*

1. El presidente desempeñará las siguientes funciones:

a) convocar las reuniones del Comité y preparar su orden del día;
b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;
c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.

2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75. *Secretaría.*

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.
2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.
3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.
4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.
5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.
6. La secretaría será responsable, en particular, de:

a) los asuntos corrientes del Comité;
b) la comunicación entre los miembros del Comité, su presidente y la Comisión;
c) la comunicación con otras instituciones y con el público;
d) la utilización de medios electrónicos para la comunicación interna y externa;
e) la traducción de la información pertinente;
f) la preparación y el seguimiento de las reuniones del Comité;
g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76. *Confidencialidad.*

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.

2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo [21].

[21] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 77. *Derecho a presentar una reclamación ante una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78. *Derecho a la tutela judicial efectiva contra una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79. *Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento.*

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80. *Representación de los interesados.*

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el

ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81. *Suspensión de los procedimientos.*

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.

2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.

3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82. *Derecho a indemnización y responsabilidad.*

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83. *Condiciones generales para la imposición de multas administrativas.*

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones del organismo de supervisión a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84. *Sanciones.*

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX

Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85. *Tratamiento y libertad de expresión y de información.*

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86. *Tratamiento y acceso del público a documentos oficiales.*

Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87. *Tratamiento del número nacional de identificación.*

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88. *Tratamiento en el ámbito laboral.*

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleadores o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 89. *Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.*

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre y cuando sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90. *Obligaciones de secreto.*

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91. *Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.*

1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.

2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X

Actos delegados y actos de ejecución

Artículo 92. *Ejercicio de la delegación.*

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. La delegación de poderes indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.

3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación

al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93. *Procedimiento de comité.*

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.
2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.
3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO XI

Disposiciones finales

Artículo 94. *Derogación de la Directiva 95/46/CE.*

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.
2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95. *Relación con la Directiva 2002/58/CE.*

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96. *Relación con acuerdos celebrados anteriormente.*

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97. *Informes de la Comisión.*

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.
2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:

a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;
b) el capítulo VII sobre cooperación y coherencia.

3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.
4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98. *Revisión de otros actos jurídicos de la Unión en materia de protección de datos.*

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99. *Entrada en vigor y aplicación.*

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

§ 6

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

Agencia Española de Protección de Datos
«BOE» núm. 296, de 12 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-21648

El incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica. Además es un sector que ofrece múltiples medios de tratar datos personales como pueden ser los circuitos cerrados de televisión, grabación por dispositivos «webcam», digitalización de imágenes o instalación de cámaras en el lugar de trabajo. Precisamente la última Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres los pasados días 1 a 3 de noviembre de este año, ha girado en torno a la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos. Todo esto hace necesario que, en ejercicio de la competencia que le atribuye el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Agencia Española de Protección de Datos dicte una Instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de dicha Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

El marco en que se mueve la presente Instrucción es claro. La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1332/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica.

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

Se excluyen de la presente Instrucción los datos personales grabados para uso o finalidad doméstica de conformidad con lo establecido en el artículo 2 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, si bien en el sentido estricto señalado por el Tribunal de Justicia de las Comunidades Europeas en la Sentencia de 6 de noviembre de 2003, asunto Lindqvist, que al interpretar la excepción prevista en el artículo 3 apartado 2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, indica que únicamente contempla «las actividades que se inscriben en el marco de la vida privada o familiar de los particulares» y no otras distintas. En la misma línea se pronuncia el Dictamen 4/2004, adoptado por el Grupo de Trabajo creado por el Artículo 29 de la Directiva 95/46/CE, con fecha 25 de noviembre de 2002.

Además, la Instrucción tampoco se aplicará al tratamiento de imágenes cuando éstas se utilizan para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad, que está cubierto por normas específicas, aunque estos tratamientos también deberán cumplir las garantías establecidas por la Ley Orgánica 15/1999.

Por otro lado, la Instrucción pretende adecuar los tratamientos a los criterios marcados por la jurisprudencia del Tribunal Constitucional al considerar que el tratamiento de datos personales no exige la conservación de los mismos, sino que basta su recogida o grabación. En el mismo sentido se han pronunciado las legislaciones que sobre esta materia han adoptado los distintos Estados miembros de la Unión Europea, cumpliendo así el mandato contenido en la Directiva 95/46/CE.

Por último, las plenas garantías de protección de los datos personales, así como las peculiaridades de su tratamiento exige una regulación concreta evitando la aplicación de un conjunto de reglas abstractas y dispersas. Por ello, a la hora de regular la legitimación del tratamiento de imágenes, la Agencia Española de Protección de Datos, entiende que es requisito esencial la aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD, sin perjuicio del estricto cumplimiento de los requisitos que para la instalación de cámaras o videocámaras de vigilancia vengan exigidos por la legislación vigente. Asimismo se regula el contenido del deber de información previsto en el artículo 5 de la misma Ley Orgánica, así como el ejercicio de los derechos a que se refieren los artículos 15 y siguientes de la citada Ley Orgánica. Por descontado, la creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispongo:

Artículo 1. *Ámbito objetivo.*

1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.

2. El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia.

3. No se considera objeto de regulación de esta Instrucción el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar.

Artículo 2. *Legitimación.*

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.

Artículo 3. *Información.*

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.

Artículo 4. *Principios de calidad, proporcionalidad y finalidad del tratamiento.*

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Artículo 5. *Derechos de las personas.*

1. Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

2. El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

3. El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

Artículo 6. *Cancelación.*

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Artículo 7. *Notificación de ficheros.*

1. La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Articulo 8. *Seguridad y Secreto.*

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

Disposición transitoria.

Los responsables de ficheros de videovigilancia ya inscritos en el Registro General de la Agencia Española de Protección de Datos deberán adoptar las medidas previstas en el artículo 3, letra a), y en el artículo 4.3 de esta Instrucción en el plazo máximo de tres meses desde su entrada en vigor.

Disposición final.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

2. El modelo a que se refiere el apartado anterior, está disponible en la página web de la Agencia Española de Protección de Datos, www.agpd.es, de donde podrá ser descargado, especificando los datos del responsable.

§ 7

Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo

Agencia de Protección de Datos
«BOE» núm. 62, de 12 de marzo de 1996
Última modificación: sin modificaciones
Referencia: BOE-A-1996-5698

La necesidad de establecer la forma de llevar los ficheros automatizados utilizados para controlar la entrada en casinos y salas de bingo obliga a precisar una serie de criterios interpretativos que faciliten la aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En concreto, es necesario regular el cumplimiento del deber de información al ciudadano en la recogida de datos personales, el consentimiento en la cesión de los datos así recabados en los supuestos en que la misma no debe efectuarse por causas legales, así como el plazo en que los datos deben ser cancelados por haber dejado de ser necesarios o pertinentes para los fines para los que se recabaron.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera. *Ámbito de aplicación.*

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados con la finalidad de controlar el acceso por las sociedades explotadoras de casinos de juego o por cualquier empresa titular de una sala de bingo.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda. *Responsable del fichero.*

1. Tendrá la consideración de responsable del fichero la sociedad explotadora del casino de juego o la empresa titular de la sala de bingo.

2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera. *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. No podrán recogerse más datos personales que aquellos estrictamente necesarios para controlar el acceso, quedando, en todo caso, limitados a los que aparecen en el documento identificador exigido para la entrada.

Norma cuarta. *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta. *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de seis meses, contado a partir de la fecha del último acceso.

Norma sexta. *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 8

Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios

Agencia de Protección de Datos
«BOE» núm. 62, de 12 de marzo de 1996
Última modificación: sin modificaciones
Referencia: BOE-A-1996-5697

La necesidad de regular los ficheros automatizados establecidos para el control del acceso de las personas a los centros de trabajo o dependencias públicas, a donde se acude con la finalidad de efectuar actividades relacionadas con las propias del centro visitado, plantea problemas relacionados con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Estos problemas se concretan en la necesidad de regular los datos constituidos por sonido e imagen, como los de vigilancia por videocámara, y, en general, todos los recopilados en cumplimiento de las funciones de vigilancia, con la prestación del consentimiento necesario para ello, así como el período en que los mismos deban ser conservados y su posterior cancelación por haber dejado de ser necesarios o pertinentes para los fines para los que fueron recabados.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera. *Ámbito de aplicación.*

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados, así como a establecimientos, espectáculos, certámenes y convenciones.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda. *Responsable del fichero.*

1. Tendrá la consideración de responsable del fichero la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo por cuya cuenta se efectúe la realización del servicio de seguridad. No obstante lo anterior, mediante el correspondiente

contrato de prestación de servicios de seguridad, podrá tener la consideración de responsable del fichero la empresa que preste los servicios de aquella naturaleza.

2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera. *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. Los datos recogidos serán los estrictamente necesarios para cumplir la finalidad de controlar el acceso.

Norma cuarta. *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta. *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados.

Norma sexta. *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 9

Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal

Agencia de Protección de Datos
«BOE» núm. 110, de 9 de mayo de 1995
Última modificación: sin modificaciones
Referencia: BOE-A-1995-10931

La concesión de un crédito hipotecario o personal, que suele ir acompañada de un seguro de vida por el importe de aquél y del que se señala como beneficiaria a la entidad de crédito de que se trate por la suma del capital no amortizado, incide sobre un importante número de disposiciones de nuestro ordenamiento jurídico.

Es obvio que la regulación jurídica de alguna de estas materias (Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios; Ley 16/1989, de 17 de julio, de Defensa de la Competencia; Ley 9/1992, de 30 de abril, de Mediación en Seguros Privados), excede de las competencias que tiene atribuidas la Agencia de Protección de Datos. Ahora bien, la precisión de si los datos son o no sensibles, con la incidencia que ello tiene en su recogida, tratamiento y cesión, la determinación del fichero en donde deban ser tratados, la de si es preciso que en esta materia, por tratarse de datos especialmente protegidos, el nivel de protección de los mismos se extienda excepcionalmente a los ficheros manuales o no automatizados, son, entre otras, cuestiones que deben ser fijadas por la Agencia de Protección de Datos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

Norma primera. *Ámbito de aplicación.*

La presente Instrucción será de aplicación a los datos personales solicitados por las entidades de crédito con motivo de la celebración de un contrato de seguro de vida anejo a la concesión de un crédito hipotecario o personal.

Norma segunda. *De la recogida de los datos.*

1. La obtención de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal, efectuada por las entidades de crédito a través de cuestionarios u otros impresos deberá realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. En los formularios cuyo destinatario sean las entidades bancarias no podrán recabarse en ningún caso datos relativos a la salud del solicitante.

2. Cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la entidad de crédito de que los datos obtenidos a tal fin solamente serán utilizados por la entidad aseguradora. Las entidades de crédito no podrán incluir los datos de salud en sus ficheros informatizados o en aquéllos en los que almacenen datos de forma convencional.

3. En ningún caso se considerará, por la naturaleza de la información solicitada o por las circunstancias en que se recaba, que se puede prescindir del derecho de la información en la recogida de los datos previstos en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Por tanto, será necesario informar previamente, en los formularios u otros impresos de recogida, de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

4. Cuando la recogida de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal efectuada por las entidades de crédito, se lleve a cabo por procedimientos distintos a los del formulario u otros impresos deberá informarse al afectado de los extremos previstos en el apartado tercero.

Norma tercera. *Consentimiento del afectado y tratamiento de los datos.*

El afectado deberá manifestar su consentimiento por separado para cada uno de los contratos y para el tratamiento distinto de la información que ambos conllevan.

Las entidades de crédito solamente podrán tratar aquellos datos personales, no especialmente protegidos, que sean estrictamente necesarios para relacionar el contrato de préstamo con el contrato de seguro de vida celebrado como consecuencia de aquél o que estén justificados por la intervención de la entidad de crédito como agente o tomador del contrato de seguro.

Norma cuarta. *Cesión de los datos.*

En ningún caso podrá considerarse que la cesión de cualquier clase de datos personales solicitados por la entidad aseguradora a la de crédito, o viceversa, se halla amparada por lo establecido en el artículo 11.2. c), de la Ley Orgánica 5/1992.

Norma transitoria. *Aplicación a contratos celebrados con anterioridad.*

Los datos de salud correspondientes a los contratos de seguro de vida celebrados con anterioridad a la publicación de esta Instrucción, que se encuentren incluidos en ficheros de las entidades de crédito, automatizados o no, deberán ser cancelados en el plazo de un mes, contado a partir de la entrada en vigor de la misma.

Norma final. *Entrada en vigor.*

La presente Instrucción entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

§ 10

Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos

Comunidad Autónoma de Cataluña
«DOGC» núm. 5731, de 8 de octubre de 2010
«BOE» núm. 257, de 23 de octubre de 2010
Última modificación: 13 de marzo de 2015
Referencia: BOE-A-2010-16136

EL PRESIDENTE DE LA GENERALIDAD DE CATALUÑA

Sea notorio a todos los ciudadanos que el Parlamento de Cataluña ha aprobado y yo, en nombre del Rey y de acuerdo con lo que establece el artículo 65 del Estatuto de autonomía de Cataluña, promulgo la siguiente Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

PREÁMBULO

La recogida y el tratamiento de información por parte de las entidades que forman el sector público, necesarios para el desarrollo de las funciones que les encomienda el ordenamiento jurídico, ha experimentado en los últimos años un considerable crecimiento, derivado no solo de la ampliación de la actividad del sector público, sino, fundamentalmente, del espectacular crecimiento de las posibilidades que ofrecen los medios tecnológicos para el tratamiento de la información. En este contexto y ante los riesgos que este fenómeno comporta, adquiere una relevancia creciente el derecho a la protección de datos, no únicamente para preservar el derecho a la intimidad, sino también, con carácter instrumental, para preservar los demás derechos de la persona reconocidos por la Constitución, el Estatuto de autonomía y el resto del ordenamiento jurídico.

El derecho a la protección de datos está reconocido por el Convenio 108, de 28 de enero de 1981, del Consejo de Europa, por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, así como por el artículo 18.4 de la Constitución española y el artículo 31 del Estatuto de autonomía. Regulado en el ámbito estatal por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el derecho a la protección de datos comporta no solo el poder jurídico de imponer a terceros el deber de abstenerse de cualquier intromisión en la esfera íntima de la persona, sino, más allá de eso, un poder de disposición sobre los datos personales que se traduce en el reconocimiento del derecho a que se requiera el consentimiento para el uso y la recogida de dichos datos personales, del derecho a ser informado, del derecho a acceder, rectificar, cancelar dichos datos y oponerse a su utilización en determinados supuestos, así como del derecho a que la recogida y el tratamiento sean realizados en condiciones que garanticen su seguridad.

La Agencia Catalana de Protección de Datos, autoridad independiente creada por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, ha velado por la garantía del derecho a la protección de datos en el ámbito de las administraciones públicas de Cataluña mediante el asesoramiento, la difusión del derecho y el cumplimiento de las funciones de control establecidas por el ordenamiento jurídico.

La aprobación del Estatuto de autonomía de 2006 supuso el reconocimiento expreso, por vez primera en el ámbito estatutario, del derecho a la protección de datos y reforzó el papel de la autoridad de control en materia de protección de datos, ya que, por una parte, clarificó y amplió su ámbito de actuación y, por otra, reforzó su independencia al establecer su designación parlamentaria.

Junto con estas exigencias derivadas del Estatuto de autonomía y otras mejoras técnicas necesarias, es preciso también incorporar a la legislación vigente en Cataluña otras modificaciones, como la propia denominación de la autoridad, para evitar la confusión de su naturaleza con el de las entidades de carácter instrumental que bajo la denominación de agencias han aparecido últimamente en el ámbito administrativo.

CAPÍTULO I

Disposiciones generales

Artículo 1. *La Autoridad Catalana de Protección de Datos.*

La Autoridad Catalana de Protección de Datos es el organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalidad, los derechos a la protección de datos personales y de acceso a la información vinculada a ellos.

Artículo 2. *Naturaleza jurídica.*

1. La Autoridad Catalana de Protección de Datos es una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

2. La Autoridad Catalana de Protección de Datos se relaciona con el Gobierno mediante el departamento que se determine por reglamento.

Artículo 3. *Ámbito de actuación.*

El ámbito de actuación de la Autoridad Catalana de Protección de Datos comprende los ficheros y los tratamientos que llevan a cabo:

a) Las instituciones públicas.

b) La Administración de la Generalidad.

c) Los entes locales.

d) Las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos.

e) Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ellos:

Primero.–Que su capital pertenezca mayoritariamente a dichos entes públicos.

Segundo.–Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos.

Tercero.–Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría.

f) Las demás entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de dichos servicios.

g) Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen.

h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña.

i) Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido por la presente ley.

Artículo 4. *Competencias.*

Para el cumplimiento de las funciones que la presente ley le asigna y dentro de su ámbito de actuación, corresponden a la Autoridad Catalana de Protección de Datos las competencias de registro, control, inspección, sanción y resolución, así como la aprobación de propuestas, recomendaciones e instrucciones.

Artículo 5. *Funciones.*

Las funciones de la Autoridad Catalana de Protección de Datos son:

a) Velar por el cumplimiento de la legislación vigente sobre protección de datos de carácter personal.

b) Resolver las reclamaciones de tutela formuladas por las personas afectadas respecto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

c) Promover, en el ámbito de sus competencias, la divulgación de los derechos de las personas con relación a la protección de datos y el acceso a la información, y la evaluación del impacto sobre la privacidad.

d) Velar por el cumplimiento de las disposiciones que la Ley 23/1998, de 30 de diciembre, de estadística de Cataluña establece respecto a la recogida de datos estadísticos y al secreto estadístico, y adoptar las medidas correspondientes para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas, sin perjuicio de las competencias atribuidas al Instituto de Estadística de Cataluña. A tales efectos, la Autoridad, en el ámbito de sus competencias, puede adoptar instrucciones y resoluciones dirigidas a los órganos administrativos y puede solicitar, si procede, la colaboración del Instituto de Estadística de Cataluña.

e) Dictar, sin perjuicio de las competencias de otros órganos e instituciones, las instrucciones y las recomendaciones en materia de protección de datos de carácter personal y de acceso a la información.

f) Requerir a los responsables del fichero o del tratamiento y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de los datos personales objeto de investigación a la legislación vigente en materia de protección de datos de carácter personal y, en su caso, ordenar el cese de los tratamientos y la supresión de los ficheros.

g) Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.

h) Atender las peticiones de información, las quejas y las denuncias.

i) Decidir sobre las inscripciones de ficheros y el tratamiento de datos de carácter personal en el Registro de Protección de Datos de Cataluña, así como tener conocimiento de los demás ficheros en que, a pesar de estar exentos del deber de inscripción en el Registro, la legislación vigente establezca un deber de comunicación a la autoridad de protección de datos.

j) Ejercer la potestad de inspección.

k) Ejercer la potestad sancionadora sobre cualquier tipo de fichero o tratamiento sometido a la normativa de protección de datos, en el ámbito que establece el artículo 3.

l) Elaborar planes de auditoría.

m) Emitir informe, con carácter preceptivo, sobre los proyectos de disposiciones de carácter general de la Generalidad de creación, modificación o supresión de ficheros de datos de carácter personal, y sobre las disposiciones que afecten a la protección de datos de carácter personal.

n) Emitir informe, con carácter potestativo, sobre los proyectos de disposiciones de carácter general de los entes locales de creación, modificación o supresión de ficheros, y

sobre las disposiciones que tengan impacto en materia de protección de datos de carácter personal que los entes locales le sometan.

o) Responder a las consultas que formulen las entidades de su ámbito de actuación sobre la protección de datos de carácter personal al poder de las administraciones públicas y colaborar con estas entidades en la difusión de las obligaciones derivadas de la legislación reguladora de estas materias.

p) Otorgar las autorizaciones para la exención del deber de información en la recogida de datos, para el mantenimiento íntegro de determinados datos y las demás autorizaciones que establece la normativa vigente en materia de protección de datos.

q) Colaborar con la Agencia Española de Protección de Datos y con las demás agencias autonómicas, de acuerdo con lo establecido por la normativa reguladora de la agencia estatal.

r) Cumplir las demás funciones que le sean atribuidas de acuerdo con las leyes.

CAPÍTULO II

Organización

Artículo 6. *Órganos de gobierno.*

Los órganos de la Autoridad Catalana de Protección de Datos son:

a) El director o directora.
b) El Consejo Asesor de Protección de Datos.

Artículo 7. *El director o directora.*

1. El director o directora de la Autoridad Catalana de Protección de Datos dirige la institución y ejerce su representación.

2. El director o directora de la Autoridad Catalana de Protección de Datos, con sujeción al ordenamiento jurídico, con plena independencia y objetividad y sin sujeción a mandato imperativo alguno ni a instrucción de ninguna clase, ejerce las funciones que establece el artículo 8 y las que se establezcan por ley o reglamento.

3. El director o directora de la Autoridad Catalana de Protección de Datos es designado por el Pleno del Parlamento por mayoría de tres quintas partes, a propuesta del Consejo Asesor de Protección de Datos, de entre personas con condición política de catalanes, con pleno uso de sus derechos civiles y políticos y con experiencia en materia de protección de datos. Si no obtiene la mayoría requerida, debe someterse a una segunda votación, en la misma sesión del Pleno, en que requiere el voto favorable de la mayoría absoluta de los miembros de la cámara.

4. Los candidatos a director o directora de la Autoridad Catalana de Protección de Datos que proponga el Consejo Asesor de Protección de Datos deben comparecer ante la correspondiente comisión del Parlamento de Cataluña para que sus miembros puedan pedir las pertinentes aclaraciones y explicaciones sobre cualquier aspecto relacionado con su formación académica, trayectoria profesional o méritos alegados.

5. El director o directora de la Autoridad Catalana de Protección de Datos es elegido por un periodo de cinco años, renovable una sola vez.

6. El director o directora de la Autoridad Catalana de Protección de Datos cesa por las siguientes causas:

a) Por expiración del plazo del mandato.
b) A petición propia.
c) Por separación, acordada por el Pleno del Parlamento por mayoría de tres quintas partes, por incumplimiento grave de sus obligaciones, incompatibilidad, incapacidad sobrevenida para el ejercicio de sus funciones declarada por sentencia firme o condena firme por delito doloso.

7. El director o directora de la Autoridad Catalana de Protección de Datos tiene la consideración de alto cargo, asimilado al de secretario o secretaria general. El cargo, sin

perjuicio del régimen de incompatibilidades de los altos cargos al servicio de la Generalidad, es incompatible con:

a) El ejercicio de cualquier mandato representativo.
b) El ejercicio de funciones directivas o ejecutivas en partidos políticos, sindicatos o asociaciones empresariales, o el estar afiliado a ellos.
c) La pertenencia al Consejo de Garantías Estatutarias o al Tribunal Constitucional.
d) El ejercicio de cualquier cargo político o función administrativa en organismos internacionales, la Unión Europea, el Estado, las comunidades autónomas o las entidades locales.
e) El ejercicio de las carreras judicial, fiscal o militar.
f) El desarrollo de cualquier actividad profesional, mercantil, industrial o laboral.

Artículo 8. *Funciones del director o directora.*

1. Corresponde al director o directora de la Autoridad Catalana de Protección de Datos dictar las resoluciones y las instrucciones y aprobar las recomendaciones y los dictámenes que requiera el ejercicio de las funciones de la Autoridad, y en especial aprobar las instrucciones a que se refiere el artículo 15.
2. Corresponden al director o directora de la Autoridad Catalana de Protección de Datos, en el ámbito específico de las competencias de la Autoridad, las siguientes funciones:

a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro de Protección de Datos de Cataluña.
b) Resolver motivadamente sobre la procedencia o improcedencia de la denegación del ejercicio de los derechos de oposición, acceso, rectificación o cancelación.
c) Requerir a los responsables y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de datos personales objeto de investigación a la legislación vigente y ordenar, si procede, el cese de los tratamientos y la cancelación de los ficheros.
d) Adoptar las medidas, resoluciones e instrucciones necesarias para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas.
e) Dictar las instrucciones y recomendaciones necesarias para adecuar los tratamientos de datos personales a los principios de la legislación vigente en materia de datos personales.
f) Emitir informe, con carácter preceptivo, de los anteproyectos de ley, de los proyectos de disposiciones normativas que elabore el Gobierno por delegación legislativa y de los proyectos de reglamentos o disposiciones de carácter general que afecten a la protección de datos de carácter personal.
g) Responder a las consultas que la Administración de la Generalidad, los entes locales y las universidades de Cataluña le formulen sobre la aplicación de la legislación de protección de datos de carácter personal.
h) Resolver sobre la adopción de medidas para corregir los efectos de las infracciones.
i) Proponer el inicio de actuaciones disciplinarias contra los responsables o los encargados del tratamiento, de acuerdo con lo establecido por la legislación vigente sobre régimen disciplinario de las administraciones públicas.
j) Resolver los expedientes sancionadores que sean de su competencia y poner en conocimiento de la Agencia Española de Protección de Datos las presuntas infracciones cuya sanción le corresponda.
k) Ordenar el cese del tratamiento, de la comunicación ilícita de datos o la inmovilización de los ficheros, cuando proceda.
l) Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.
m) Cumplir las funciones con relación a los planes de auditoría de la Autoridad a que se refiere el artículo 20.
n) Atender las peticiones que le formulen los ciudadanos.
o) Responder a las consultas que le formulen las administraciones.

p) Elaborar la memoria anual de las actuaciones y actividades de la Autoridad a que se refiere el artículo 13 y comparecer ante la comisión pertinente del Parlamento para informar de su contenido.
q) Cumplir cualquier otra que le sea encomendada por ley o reglamento.

3. Corresponden al director o directora de la Autoridad Catalana de Protección de Datos, en los ámbitos económico, de contratación y de recursos humanos de la Autoridad, las siguientes funciones:

a) Adjudicar y formalizar los contratos que requiera la gestión de la Autoridad y vigilar su cumplimiento y ejecución.
b) Aprobar los gastos y ordenar los pagos, dentro de los límites de los créditos del presupuesto de gastos de la Autoridad.
c) Elaborar el anteproyecto de presupuesto de la Autoridad y someterlo a la consideración del Consejo Asesor de Protección de Datos.
d) Aprobar la plantilla de personal de la Autoridad.

Artículo 9. *El Consejo Asesor de Protección de Datos.*

1. El Consejo Asesor de Protección de Datos es el órgano de asesoramiento y participación de la Autoridad Catalana de Protección de Datos y está constituido por los siguientes miembros:

a) El presidente o presidenta, que es nombrado por el Consejo de entre sus miembros, una vez efectuada la renovación ordinaria de los miembros designados por el Parlamento.
b) Tres personas designadas por el Parlamento, por mayoría de tres quintas partes. Si no obtienen la mayoría requerida, deben someterse a una segunda votación, en la misma sesión del Pleno, en que se requiere el voto favorable de la mayoría absoluta.
c) Tres personas en representación de la Administración de la Generalidad, designadas por el Gobierno.
d) Dos personas en representación de la Administración local de Cataluña, designadas por el Consejo de Gobiernos Locales.
e) Una persona experta en el ámbito de los derechos fundamentales, designada por el Consejo Interuniversitario de Cataluña.
f) Una persona experta en informática, designada por el Consejo Interuniversitario de Cataluña.
g) Una persona designada por el Instituto de Estudios Catalanes.
h) Una persona en representación de las organizaciones de consumidores y usuarios, designada por el Consejo de las Personas Consumidoras de Cataluña.
i) El director o directora del Instituto de Estadística de Cataluña.
j) Un funcionario o funcionaria de la Autoridad Catalana de Protección de Datos, que actúa de secretario o secretaria del Consejo.

2. La renovación de los miembros del Consejo Asesor de Protección de Datos se lleva a cabo cada cinco años de acuerdo con los estatutos de la Autoridad Catalana de Protección de Datos.
3. El director o directora de la Autoridad Catalana de Protección de Datos asiste a las reuniones del Consejo Asesor de Protección de Datos con voz y sin voto.

Artículo 10. *Funciones del Consejo Asesor de Protección de Datos.*

1. Las funciones del Consejo Asesor de Protección de Datos son:

a) Proponer al Parlamento la persona o personas candidatas a ocupar el puesto de director o directora de la Autoridad.
b) Emitir informe sobre los proyectos de instrucciones de la Autoridad que le sean sometidos.
c) Emitir informe sobre el anteproyecto de presupuesto anual de la Autoridad que el director o directora proponga.
d) Asesorar al director o directora de la Autoridad sobre cuantas cuestiones le sean sometidas.

e) Elaborar un informe preceptivo previo a la aprobación de la plantilla del personal de la Autoridad.
f) Elaborar un informe vinculante sobre el número máximo de trabajadores de la plantilla de personal eventual de la Autoridad.
g) Elaborar estudios y propuestas en materia de protección de datos de carácter personal y pedir al director o directora el establecimiento de criterios en la materia.

2. El Consejo Asesor de Protección de Datos ha de ser informado de:

a) La actividad de la Autoridad Catalana de Protección de Datos, por parte del director o directora y de forma periódica.
b) La memoria anual de la Autoridad.
c) Los criterios objetivos de los planes de auditoría a que se refiere el artículo 20.

3. El Consejo Asesor de Protección de Datos se rige por las normas que se establezcan por reglamento y, supletoriamente, por las disposiciones vigentes sobre funcionamiento de órganos colegiados de la Administración de la Generalidad.

Artículo 11. *El Registro de Protección de Datos de Cataluña.*

1. El Registro de Protección de Datos de Cataluña se integra en la Autoridad Catalana de Protección de Datos.
2. Son objeto de inscripción en el Registro de Protección de Datos de Cataluña:

a) Los ficheros de datos personales, de titularidad pública o privada, incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos.
b) Los códigos tipo formulados por las entidades incluidas dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos.
c) Las autorizaciones de tratamientos de datos de carácter personal previstas en la legislación vigente.

3. El Gobierno debe establecer por reglamento el procedimiento de inscripción de la creación, la modificación y la supresión de ficheros en el Registro de Protección de Datos de Cataluña, así como el contenido de los asientos registrales.
4. El Registro de Protección de Datos de Cataluña es de consulta pública y gratuita. Cualquier persona puede consultar, como mínimo, la información sobre la existencia de un determinado tratamiento de datos de carácter personal, las finalidades y la identidad de la persona responsable del tratamiento.
5. La Autoridad Catalana de Protección de Datos debe establecer los acuerdos de cooperación necesarios con la Agencia Española de Protección de Datos para integrar la información registral y mantenerla actualizada.

CAPÍTULO III

Relaciones con otros organismos e instituciones

Artículo 12. *Colaboración con otras instituciones.*

La Autoridad Catalana de Protección de Datos puede suscribir convenios de colaboración con el Síndic de Greuges, los síndicos locales, el Instituto de Estadística de Cataluña, las universidades y otras instituciones y organismos de defensa de los derechos de las personas.

Artículo 13. *Memoria anual.*

1. La Autoridad Catalana de Protección de Datos debe elaborar una memoria anual de sus actividades y de las conclusiones de los trabajos y expedientes que ha tramitado.
2. La Autoridad Catalana de Protección de Datos debe presentar la memoria anual en el Parlamento y dar cuenta de la misma en el marco de la comisión correspondiente, y remitirla también al Gobierno, al Síndic de Greuges y al director o directora de la Agencia Española de Protección de Datos.

Artículo 14. *Relaciones entre la Autoridad Catalana de Protección de Datos y el Síndic de Greuges.*

Las relaciones entre la Autoridad Catalana de Protección de Datos y el Síndic de Greuges son de colaboración en el ámbito de sus respectivas competencias.

CAPÍTULO IV

Ejercicio de competencias y funciones

Artículo 15. *Instrucciones.*

1. El director o directora de la Autoridad Catalana de Protección de Datos puede aprobar instrucciones para la adecuación de los ficheros y los tratamientos de datos a los principios y garantías que establece la legislación vigente en materia de protección de datos.
2. El proyecto de instrucción debe someterse a información pública y a informe del Consejo Asesor de Protección de Datos. Igualmente, puede ser sometido a informe de la Comisión Jurídica Asesora.
3. Las instrucciones a que se refiere el apartado 1 se publican en el «Diari Oficial de la Generalitat de Catalunya» y en la sede electrónica de la Autoridad Catalana de Protección de Datos.

Artículo 16. *Tutela de los derechos de acceso, rectificación, oposición y cancelación.*

1. Las personas interesadas a las que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, de rectificación, de cancelación o de oposición, o que puedan entender desestimada su solicitud por el hecho de no haber sido resuelta y remitida dentro del plazo establecido, pueden presentar una reclamación ante la Autoridad Catalana de Protección de Datos.
2. La Autoridad Catalana de Protección de Datos debe resolver expresamente sobre la procedencia o improcedencia de la reclamación a que se refiere el apartado 1 en el plazo de seis meses, previa audiencia de la persona responsable del fichero así como de las personas interesadas si el resultado del primer trámite de audiencia lo hace necesario. Transcurrido dicho plazo sin que la Autoridad notifique la resolución, se entiende que ha sido desestimada.
3. La resolución de estimación total o parcial de la tutela de un derecho ha de establecer el plazo en que este debe hacerse efectivo.
4. Si la solicitud de ejercicio del derecho ante la persona responsable del fichero es estimada, total o parcialmente, pero el derecho no se ha hecho efectivo en la forma y los plazos exigibles de acuerdo con la normativa aplicable, las personas interesadas pueden ponerlo en conocimiento de la Autoridad Catalana de Protección de Datos para que se lleven a cabo las correspondientes actuaciones sancionadoras.

Artículo 17. *Publicidad de los informes y resoluciones.*

1. La Autoridad Catalana de Protección de Datos está obligada a garantizar la confidencialidad de las consultas y reclamaciones de que tenga conocimiento, sin perjuicio del derecho de acceso a la información y documentación administrativas de las personas interesadas.
2. Los dictámenes, informes y resoluciones de la Autoridad Catalana de Protección de Datos deben hacerse públicos, una vez notificados a las personas interesadas, previa «anonimización» de los datos de carácter personal, sin perjuicio de lo establecido por el apartado 1.
3. De forma excepcional, puede optarse por no publicar las resoluciones sin interés doctrinal alguno o que, pese a la «anonimización», sea aconsejable por causas justificadas evitar su publicidad para impedir hacer reconocibles a las personas que lo solicitan.

Artículo 18. *Funciones de control.*

1. La actividad de control de la Autoridad Catalana de Protección de Datos se lleva a cabo mediante la potestad de inspección, los planes de auditoría, la aplicación del régimen sancionador, los requerimientos de adecuación a la legalidad y la potestad de inmovilización de ficheros.

2. Los hechos constatados por los funcionarios al servicio de la Autoridad Catalana de Protección de Datos al llevar a cabo su tarea de control e inspección, si sus actuaciones se formalizan en un documento público en que se observen los requisitos legales pertinentes, tienen valor probatorio, sin perjuicio de las pruebas en defensa de los respectivos derechos o intereses que puedan aportar los propios interesados.

Artículo 19. *Potestad de inspección.*

1. La Autoridad Catalana de Protección de Datos puede inspeccionar los ficheros y los tratamientos de datos personales a que se refiere la presente ley, a fin de obtener todas las informaciones necesarias para el ejercicio de sus funciones. A tal fin, la Autoridad puede solicitar la presentación o la remisión de documentos y de datos o examinarlos en el lugar donde estén depositados, así como inspeccionar los equipos físicos y lógicos utilizados, para lo cual puede acceder a los locales donde estén instalados.

2. Los funcionarios que ejercen la función inspectora a que se refiere el apartado 1 tienen la consideración de autoridad pública en el desarrollo de su actividad y quedan obligados a mantener el secreto sobre las informaciones que conozcan en el ejercicio de las funciones inspectoras, incluso después de haber cesado en las mismas.

3. En el ejercicio de las funciones de inspección los funcionarios pueden ser auxiliados por personal no funcionario, si así lo decide el director o directora de la Autoridad, en función de los conocimientos de orden técnico que puedan ser necesarios para auditar sistemas de información durante las tareas de investigación. El personal no funcionario que participa en la actividad inspectora debe hacerlo siguiendo las instrucciones y bajo la supervisión del personal funcionario inspector, y tiene las mismas obligaciones que este, especialmente en cuanto al deber de secreto.

4. Las entidades comprendidas dentro del ámbito de aplicación de la presente ley tienen la obligación de auxiliar, con carácter preferente y urgente, a la Autoridad Catalana de Protección de Datos en sus investigaciones, si esta lo solicita.

Artículo 20. *Planes de auditoría.*

1. Los planes de auditoría de la Autoridad Catalana de Protección de Datos constituyen un sistema de control preventivo para:

a) Verificar el cumplimiento de la normativa en materia de protección de datos de carácter personal.

b) Recomendar o requerir a los responsables de los ficheros y de los tratamientos de datos de carácter personal la adopción de las medidas correctoras adecuadas.

2. Corresponde al director o directora de la Autoridad Catalana de Protección de Datos:

a) Decidir el contenido de cada plan de auditoría y concretar los aspectos y tratamientos que deben ser analizados.

b) Seleccionar las entidades que deben ser objeto de los planes de auditoría mediante criterios objetivos que han de ser públicos.

3. Las entidades a que se refiere la letra b del apartado 2 deben colaborar con la persona responsable de la auditoría facilitando la realización de las verificaciones oportunas y aportando la información y documentación necesarias.

4. Las conclusiones de los planes de auditoría sobre el grado general de cumplimiento y las recomendaciones generales pertinentes deben difundirse públicamente.

5. Si durante el proceso de ejecución de un plan de auditoría la entidad afectada es objeto, previa denuncia, de la incoación de un expediente sancionador por parte de la Autoridad Catalana de Protección de Datos como consecuencia de la comisión de una posible infracción por algún aspecto coincidente o directamente relacionado con el contenido

del plan de auditoría que se está llevando a cabo, la entidad debe ser excluida del plan de auditoría y debe continuarse la tramitación del procedimiento sancionador.

6. Los requerimientos a que se refiere la letra b del apartado 1 deben establecer un plazo adecuado para la adopción de las medidas correctoras necesarias por parte de las entidades afectadas. Transcurrido dicho plazo sin que la entidad afectada informe a la Autoridad Catalana de Protección de Datos sobre las medidas adoptadas, o si estas son insuficientes o inadecuadas, la Autoridad puede iniciar las actuaciones inspectoras oportunas para incoar, si procede, un procedimiento sancionador.

Artículo 21. *Régimen sancionador.*

1. Los responsables de los ficheros y de los tratamientos de datos personales incluidos dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos y los encargados de los correspondientes tratamientos quedan sujetos al régimen sancionador establecido por la legislación estatal de protección de datos de carácter personal. Las referencias a la Agencia Española de Protección de Datos o a sus órganos, en cuanto al régimen de infracciones, deben entenderse hechas a la Autoridad Catalana de Protección de Datos o a sus órganos, en lo concerniente a su ámbito competencial.

2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos. Además, puede proponer, si procede, la iniciación de actuaciones disciplinarias de acuerdo con lo establecido por la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. Dicha resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependan y a las personas afectadas, si las hay.

3. En el caso de infracciones cometidas con relación a ficheros de titularidad privada, la resolución que declare la infracción debe imponer las sanciones previstas por la legislación de protección de datos y las medidas a adoptar para corregir los efectos de la infracción.

4. El director o directora de la Autoridad Catalana de Protección de Datos debe informar al síndic o síndica de greuges de las actuaciones que haga a consecuencia de una solicitud del mismo y debe comunicarle las resoluciones sancionadoras que dicte con relación a dichas actuaciones.

Artículo 22. *Procedimiento sancionador.*

1. El Gobierno debe establecer por decreto el procedimiento para la determinación de las infracciones y la imposición de sanciones.

2. La denuncia que inicia un procedimiento sancionador debe formalizarse mediante escrito razonado y estar debidamente firmada.

3. La persona denunciante debe identificarse en el momento de hacer la denuncia a que se refiere el apartado 2. Sin embargo, puede solicitar de forma razonada que su identidad no sea revelada, previa ponderación de los intereses en conflicto por la Autoridad Catalana de Protección de Datos, cuando haya motivos fundamentados y legítimos relativos a una situación personal concreta que así lo justifique.

4. La persona denunciante tiene derecho a que le sean comunicadas las actuaciones que se deriven de su denuncia, sin perjuicio de los derechos que puedan corresponderle si también es persona interesada.

Artículo 23. *Medidas provisionales.*

En el momento de la incoación o durante la tramitación del procedimiento sancionador, el director o directora de la Autoridad Catalana de Protección de Datos puede adoptar, de forma motivada, las medidas provisionales que considere necesarias para asegurar la eficacia de la resolución que finalmente pueda recaer y para conseguir la protección provisional del derecho a la protección de datos de las personas afectadas. Con carácter previo, la Autoridad debe dar audiencia a las entidades afectadas, excepto si concurren circunstancias de urgencia que puedan hacer perder la finalidad de la medida. La resolución que adopte la medida es susceptible de los recursos procedentes.

Artículo 24. *Cumplimiento de la resolución del procedimiento sancionador.*

1. En las infracciones declaradas respecto a ficheros de titularidad pública, las personas o entidades que hayan sido declaradas responsables de la infracción deben comunicar a la Autoridad Catalana de Protección de Datos, en el plazo que establece la resolución, la adopción de las medidas y actuaciones a que se refiere el apartado 2 del artículo 25.

2. En las sanciones impuestas por infracciones cometidas respecto a ficheros de titularidad privada, el cumplimiento de la sanción debe llevarse a cabo en el plazo establecido por la legislación vigente. Dentro de este plazo, la entidad sancionada puede solicitar, de forma razonada, el fraccionamiento del pago. El director o directora de la Autoridad Catalana de Protección de Datos debe resolver la solicitud, de acuerdo con lo establecido por la normativa reguladora de la recaudación de los ingresos públicos.

3. Las personas o entidades sancionadas a quienes se haya impuesto alguna medida correctora de acuerdo con lo establecido por el artículo 25 deben comunicar a la Autoridad Catalana de Protección de Datos, en el plazo que establece la resolución, las medidas adoptadas.

Artículo 25. *Requerimientos de adecuación y potestad de inmovilización.*

1. En los supuestos, constitutivos de infracción muy grave, de utilización o de comunicación ilícita de datos personales en que se atente gravemente contra los derechos fundamentales y las libertades públicas de los ciudadanos o se impida su ejercicio, el director o directora de la Autoridad Catalana de Protección de Datos puede exigir a los responsables de los ficheros de datos personales el cese de la utilización o comunicación ilícita de datos personales.

2. Si el requerimiento a que se refiere el apartado 1 no es atendido, el director o directora de la Autoridad Catalana de Protección de Datos puede, mediante resolución motivada, inmovilizar los ficheros de datos personales, con la única finalidad de restaurar los derechos de las personas afectadas. En este supuesto, la inmovilización queda sin efecto de no acordar la Autoridad, en el plazo de quince días, la incoación de un procedimiento sancionador y ratificarse la medida.

CAPÍTULO V

Régimen jurídico, de personal, económico y de contratación

Artículo 26. *Régimen jurídico.*

1. La Autoridad Catalana de Protección de Datos, en el ejercicio de sus funciones, actúa de conformidad con lo dispuesto por la presente ley, sus disposiciones de desarrollo y la legislación reguladora del régimen jurídico de las administraciones públicas y el procedimiento administrativo aplicable a la Administración de la Generalidad.

2. Las resoluciones del director o directora de la Autoridad Catalana de Protección de Datos agotan la vía administrativa y son susceptibles de recurso contencioso-administrativo, sin perjuicio de los recursos administrativos que procedan.

Artículo 27. *Régimen de personal.*

1. La Autoridad Catalana de Protección de Datos, en el ejercicio de su potestad de autoorganización y de acuerdo con los créditos consignados en los presupuestos de la Generalidad, aprueba la relación de puestos de trabajo de los órganos y servicios que la integran y que han de ser ocupados por personal funcionario, laboral o eventual, e informa de ello al Parlamento.

2. Al personal al servicio de la Autoridad Catalana de Protección de Datos se le aplica a todos los efectos la normativa que regula el estatuto del personal al servicio de la Administración de la Generalidad en cuanto al régimen y la normativa de ordenación de la ocupación pública.

3. Los puestos de trabajo que comportan el ejercicio de potestades públicas se reservan a personal funcionario.

4. Los puestos de trabajo considerados de confianza o de asesoramiento especial no reservado a personal funcionario y que figuran con este carácter en la correspondiente relación de puestos de trabajo son desempeñados por personal eventual, cuyo número máximo fija el Consejo Asesor de Protección de Datos.

5. La Autoridad Catalana de Protección de Datos ejerce la potestad disciplinaria respecto al personal al servicio de la institución.

6. El personal al servicio de la Autoridad Catalana de Protección de Datos tiene el deber de secreto sobre las informaciones que conozca en el ejercicio de sus funciones, incluso después de haber cesado en su ejercicio.

Artículo 28. *Régimen económico y de contratación.*

1. Para el cumplimiento de sus finalidades, la Autoridad Catalana de Protección de Datos cuenta con los siguientes bienes y recursos económicos:

a) Las asignaciones anuales de los presupuestos de la Generalidad.

b) Los bienes y derechos que constituyen su patrimonio, así como los productos y rentas de los mismos.

c) El producto de las sanciones que imponga en el ejercicio de sus competencias.

d) El producto de las tasas y demás ingresos públicos devengados por su actividad.

e) Cualquier otro recurso económico que legalmente se le pueda atribuir.

2. **(Derogado).**

3. La Autoridad Catalana de Protección de Datos debe elaborar su propuesta de anteproyecto de presupuesto de ingresos y de gastos de acuerdo con las normas que dicte el departamento competente en materia de economía y finanzas para elaborar los presupuestos de la Generalidad, y debe remitirlo al departamento mediante el que se relaciona con el Gobierno para que este, sobre la base de esta propuesta, formule el anteproyecto y tramite su inclusión en el proyecto de ley de presupuestos de la Generalidad.

4. La Autoridad Catalana de Protección de Datos está sometida al control financiero de la Intervención General de la Generalidad y al régimen de contabilidad pública.

5. El régimen jurídico de contratación de la Autoridad Catalana de Protección de Datos es el establecido por la legislación sobre contratos del sector público.

6. El régimen patrimonial de la Autoridad Catalana de Protección de Datos es el establecido por la normativa que regula el patrimonio de la Administración de la Generalidad.

Disposición transitoria primera. *Sucesión de la Agencia Catalana de Protección de Datos.*

1. La Autoridad Catalana de Protección de Datos se subroga en la posición jurídica de la Agencia Catalana de Protección de Datos en cuanto a los bienes, derechos y obligaciones de cualquier tipo de que fuera titular la Agencia.

2. Las referencias hechas en el ordenamiento jurídico a la Agencia Catalana de Protección de Datos deben entenderse hechas a la Autoridad Catalana de Protección de Datos.

Disposición transitoria segunda. *Procedimiento sancionador.*

Mientras el Gobierno no apruebe el decreto que regula el procedimiento sancionador en materia de protección de datos, continúa siendo aplicable el procedimiento establecido por el Decreto 278/1993, de 9 de noviembre, sobre procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad.

Disposición transitoria tercera. *Vigencia del Estatuto de la Agencia Catalana de Protección de Datos.*

Mientras no entren en vigor los estatutos de la Autoridad Catalana de Protección de Datos, sigue siendo de aplicación, en todo lo que no se oponga a la presente ley, el Estatuto de la Agencia Catalana de Protección de Datos, aprobado por el Decreto 48/2003, de 20 de febrero.

Disposición derogatoria.

Queda derogada la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

Disposición final primera. *Estatutos de la Autoridad.*

En el plazo de seis meses a contar desde la entrada en vigor de la presente ley, el Gobierno debe aprobar los estatutos de la Autoridad Catalana de Protección de Datos.

Disposición final segunda. *Desarrollo de los procedimientos.*

Se habilita al Gobierno para la regulación de los procedimientos necesarios para el ejercicio de las funciones atribuidas a la Autoridad Catalana de Protección de Datos, sin perjuicio de la competencia de la Autoridad para concretar mediante instrucción aquellos aspectos en que sea necesario.

Disposición final tercera. *Creación, modificación y supresión de ficheros.*

1. Los consejeros de la Generalidad, dentro del ámbito de sus respectivas competencias, quedan habilitados para crear, modificar y suprimir, mediante orden, los ficheros de sus departamentos o de los entes públicos vinculados a ellos o que dependan de los mismos y los ficheros de los consorcios en que la representación de la Administración de la Generalidad en los órganos de gobierno sea mayoritaria.
2. Las entidades de derecho público dotadas de especial independencia o autonomía quedan habilitadas para ejercer la competencia de crear, modificar y suprimir ficheros.

§ 11

Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos

Comunidad Autónoma del País Vasco
«BOPV» núm. 44, de 4 de marzo de 2004
«BOE» núm. 279, de 19 de noviembre de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-18151

Se hace saber a todos los ciudadanos y ciudadanas de Euskadi que el Parlamento Vasco ha aprobado la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

EXPOSICIÓN DE MOTIVOS

Los avances de la técnica se han acelerado en los últimos tiempos. Actualmente, el uso de la informática permite tratar gran cantidad de datos relativos a las personas físicas, pudiendo llegar a conocer aspectos relacionados con las mismas que suponen una intromisión en su intimidad. Los ordenamientos jurídicos no pueden permanecer insensibles ante la eventualidad de usos perversos de las posibilidades tecnológicas, en detrimento de espacios que deben quedar reservados a la intimidad personal.

Esta tensión entre tecnología, especialmente en el campo de la informática, e intimidad de las personas apela a una actuación legislativa que procure un equilibrio satisfactorio entre dos bienes dignos de protección jurídica. Por un lado, no es bueno para la sociedad poner freno al desarrollo tecnológico, cuyas potencialidades son inmensas y deben contribuir a un mayor bienestar de la comunidad; pero, por otro, los ciudadanos tienen derecho a que se les proteja su intimidad personal, evitando que las posibilidades que ofrece la tecnología informática actual reduzcan aquélla más allá de lo deseable. Para ello es preciso limitar el uso de la informática y, de este modo, garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Es éste un mandato que el artículo 18.4 de la Constitución impone al legislador, y que éste recoge en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La preocupación por la protección de la intimidad personal y familiar de los ciudadanos, con la consiguiente limitación del uso de la informática a tal fin, no es exclusiva del legislador estatal. También las instituciones de la Unión Europea han mostrado su sensibilidad en este sentido.

El Tratado de Amsterdam de 17 de junio de 1997 ha incorporado al tratado constitutivo de la Comunidad Europea su actual artículo 286, que requiere que se apliquen a las instituciones y organismos comunitarios los actos comunitarios relativos a la protección de

las personas respecto al tratamiento de datos personales y a la libre circulación de estos datos.

Ya anteriormente, el Parlamento Europeo y el Consejo habían adoptado la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, donde se recoge el principio de que los sistemas de tratamiento de datos están al servicio del hombre y que deben respetar las libertades y derechos fundamentales de las personas físicas, en particular la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios y al bienestar de los individuos.

Según esta directiva, las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los citados derechos y libertades, particularmente el derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario, y considera que la aproximación de dichas legislaciones debe tener por objeto asegurar un alto nivel de protección.

Para la citada directiva, un elemento esencial de la protección de las personas, en lo que respecta a la protección de los datos personales, es la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros, la cual debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención.

La directiva da a los estados miembros un plazo de tres años para la adopción de las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma.

La actuación de las instituciones comunitarias en materia de protección de datos no se ha limitado a las directivas destinadas a los estados miembros, sino que también han adoptado medidas destinadas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, mediante el Reglamento (CE) número 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, el cual incluso instituye una autoridad de control independiente (el Supervisor Europeo de Protección de Datos).

Podría decirse que la garantía de un elevado nivel de protección de los datos personales y de la intimidad es un principio inspirador de la normativa comunitaria, que tiene su proyección incluso en propuestas de directiva cuya finalidad no es propiamente la regulación de la protección de los datos de carácter personal, como es el caso de la propuesta de directiva del Parlamento Europeo y del Consejo relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Diario Oficial núm. C 365 E de 19/12/2000).

En el Derecho interno, la protección de datos de carácter personal se halla regulada, como decíamos antes, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que, además de otras materias vinculadas con el derecho fundamental al que se refiere el artículo 18.4 de la Constitución, regula los aspectos básicos del régimen jurídico de la Agencia de Protección de Datos, que es la que se configura como la autoridad de control independiente a la que se refiere la Directiva 95/46/CE.

La ley orgánica establece que la mayor parte de las funciones asignadas a la citada agencia, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las comunidades autónomas y por la Administración local de su ámbito territorial, serán ejercidas por los órganos correspondientes de cada comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido. Criterio legal que es acorde con el artículo 28 de la Directiva 95/46/CE, según el cual los estados miembros dispondrán de una o más autoridades públicas que se encargarán de vigilar la aplicación, en su territorio, de las disposiciones adoptadas por ellos de acuerdo con la citada directiva, y añade que dichas autoridades ejercerán las funciones que les son atribuidas con total independencia.

Desde el punto de vista de su ordenación sistemática, la ley se halla dividida en tres títulos.

En el título I, de disposiciones generales, se concretan el objeto y el ámbito de aplicación de la ley, delimitando los ficheros que quedan bajo su regulación atendiendo a la Administración pública, institución o corporación que los crea o gestiona. La citada delimitación se completa con la enumeración de los ficheros a los que no se aplicará la ley y de aquellos en los que ésta será de aplicación limitada, por tener regímenes específicos. Contiene también una lista de definiciones muy útil para precisar y unificar la terminología específica de la materia objeto de regulación; se regulan aspectos relacionados con la creación, modificación y supresión de ficheros, limitaciones a la recogida de datos de carácter personal, información a los interesados y seguridad de los ficheros de datos, así como el procedimiento de reclamación ante la Agencia Vasca de Protección de Datos. Se trata de un título necesario para dar coherencia sistemática e integridad a la ley, que requerirá de un desarrollo posterior.

En el título II se crea la Agencia Vasca de Protección de Datos y se regulan los aspectos fundamentales de su régimen jurídico. Contiene preceptos relativos al régimen del personal a su servicio, recursos económicos, régimen presupuestario, órganos de gobierno, funciones y potestades. Es de resaltar la creación del Registro de Protección de Datos como órgano necesario de la agencia.

El título III está dedicado al régimen sancionador. En él se delimitan los sujetos responsables, se tipifican las infracciones y se establecen las sanciones correspondientes. Como dice el Reglamento (CE) número 45/2001, antes citado, un sistema de protección de datos personales requiere establecer derechos y obligaciones, pero también sanciones apropiadas para los infractores. En nuestro caso, dadas las características especiales de los titulares de los ficheros, se presta especial atención al supuesto de infracciones cometidas por el personal al servicio de las administraciones, instituciones y corporaciones a cuyos ficheros se aplica la ley.

La ley contiene tres disposiciones adicionales, relativas a la necesaria comunicación de los ficheros existentes a la Agencia Vasca de Protección de Datos, a la utilización de los datos del padrón municipal por las administraciones autonómica y forales para el ejercicio de sus competencias, y al necesario respeto de las competencias del Ararteko y de la Agencia de Protección de Datos del Estado.

Concluye con una disposición final, en la que se autoriza al Gobierno Vasco para su desarrollo y aplicación.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente ley tiene por objeto:

1. La regulación de los ficheros de datos de carácter personal creados o gestionados por la Comunidad Autónoma del País Vasco, los órganos forales de los territorios históricos y las administraciones locales de la Comunidad Autónoma del País Vasco.

2. La creación y regulación de la Agencia Vasca de Protección de Datos.

Artículo 2. *Ámbito de aplicación.*

1. La presente ley será aplicable a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, por:

a) La Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público.

b) El Parlamento Vasco.

c) El Tribunal Vasco de Cuentas Públicas.

d) El Ararteko.

e) El Consejo de Relaciones Laborales.
f) El Consejo Económico y Social.
g) El Consejo Superior de Cooperativas.
h) La Agencia Vasca de Protección de Datos.
i) La Comisión Arbitral.
j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco.
k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario.

2. No obstante lo dispuesto en el número anterior, esta ley no será de aplicación a los ficheros:

a) Sometidos a la normativa sobre protección de materias clasificadas.
b) Establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.
c) Regulados por la legislación de régimen electoral.
d) Procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por los cuerpos de Policía del País Vasco, de conformidad con la legislación sobre la materia.

3. Se regirán por sus disposiciones específicas y, en su caso, por lo especialmente previsto en esta ley los tratamientos de datos personales que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación sobre la función estadística pública.
4. Las instituciones y centros sanitarios de carácter público y los profesionales a su servicio podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con lo dispuesto en la legislación sectorial sobre sanidad, sin perjuicio de la aplicación de lo dispuesto en esta ley en todo lo que no sea incompatible con aquella legislación.
5. La aplicación de lo dispuesto en esta ley a los ficheros de datos de carácter personal, distintos de los citados en el número 2 de este artículo, creados o gestionados por los cuerpos de Policía del País Vasco se efectuará sin perjuicio de las especificidades de su régimen jurídico previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 4/1992, de 17 de julio, de Policía del País Vasco.

Artículo 3. *Definiciones.*

A los efectos de esta ley se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. Se considerará identificable toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona, institución, entidad, corporación u órgano administrativo al que está adscrito el fichero y que decide sobre la finalidad, contenido y uso del tratamiento. La disposición por la que se cree el fichero determinará el responsable del mismo. Sus funciones serán las establecidas en el documento de seguridad.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere la letra c) de este artículo.
f) Encargado del tratamiento: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

g) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que la conciernen.

h) Cesión o comunicación de datos: toda revelación de datos realizada a persona distinta del interesado.

Artículo 4. *Creación, modificación y supresión de ficheros.*

1. La creación, modificación y supresión de ficheros de la Administración de la Comunidad Autónoma se realizará por orden del titular del departamento al que esté adscrito el fichero, la cual deberá contener todas las menciones exigidas por la legislación en vigor y será objeto de publicación en el «Boletín Oficial del País Vasco». El procedimiento de elaboración de la citada orden será el previsto para la elaboración de disposiciones de carácter general.

2. En el caso de ficheros de datos de carácter personal de otras administraciones, instituciones o corporaciones, el acuerdo o disposición por la que se cree, modifique o suprima deberá contener todas las menciones exigidas y será publicada en el «Boletín Oficial del País Vasco» o del territorio histórico, según sea el ámbito territorial al que se extienden sus funciones o competencias.

Artículo 5. *Recogida de datos de carácter personal.*

Las administraciones públicas y demás instituciones, corporaciones y entidades a que se refiere el artículo 2.1 de esta ley sólo podrán recoger datos de carácter personal para su tratamiento cuando sean adecuados, pertinentes y no excesivos para el ejercicio de las respectivas competencias que tienen atribuidas. Salvo precepto legal en sentido contrario, para la obtención de dichos datos no será preciso recabar el consentimiento de los afectados, pero sólo podrán utilizarse para las finalidades determinadas, explícitas y legítimas para las que se hubieran obtenido, sin perjuicio de su posible tratamiento posterior para fines históricos, estadísticos o científicos, de acuerdo con la legislación aplicable.

Artículo 6. *Información a los interesados.*

Los interesados a los que se soliciten datos de carácter personal serán previamente informados, de conformidad con la legislación sobre protección de dichos datos. No obstante, cuando los datos no hayan sido recabados del propio interesado y la información a éste resulte imposible o exija esfuerzos desproporcionados, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, el director de la Agencia Vasca de Protección de Datos, de acuerdo con la susodicha legislación, podrá dispensar al responsable del fichero de la obligación de informar a los interesados.

Artículo 7. *Aprobación del contenido mínimo del documento de seguridad.*

En el ejercicio de sus potestades de autoorganización, los órganos de gobierno de las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley podrán aprobar, en aplicación de los preceptos relativos a la seguridad de los datos y para aplicar a todos o parte de los ficheros de los que son titulares sus respectivas administraciones, instituciones o corporaciones, el contenido mínimo del documento de seguridad que, en todo caso, deberán elaborar e implantar los responsables de fichero para garantizar la seguridad de los datos de carácter personal contenidos en los citados ficheros.

Artículo 8. *Procedimiento para el ejercicio de los derechos de los interesados.*

1. Los interesados podrán ejercitar los derechos de oposición, acceso, rectificación, cancelación y cualesquiera otros que les reconozca la ley. El contenido material de los mismos será el determinado en la ley.

2. Cada administración, institución o corporación regulará reglamentariamente el procedimiento para el ejercicio de los derechos señalados en el número anterior, en relación

con los ficheros de su titularidad a los que es de aplicación esta ley. No se exigirá contraprestación alguna por ello.

Artículo 9. *Reclamaciones ante la Agencia Vasca de Protección de Datos.*

1. Las actuaciones contrarias a lo dispuesto en esta ley pueden ser objeto de reclamación por los interesados ante la Agencia Vasca de Protección de Datos, en la forma que reglamentariamente se determine.
2. El interesado al que se deniegue, total o parcialmente, el ejercicio del derecho de oposición, acceso, rectificación, cancelación o cualquier otro que le reconozca la legislación sobre protección de datos de carácter personal, podrá ponerlo en conocimiento de la Agencia Vasca de Protección de Datos, que deberá asegurarse de la procedencia o improcedencia de la denegación.
3. El plazo máximo en que se debe dictar y notificar la resolución expresa de tutela de derechos es de seis meses, entendiéndose el silencio administrativo como desestimatorio de la tutela pedida.
4. Contra las resoluciones de la Agencia Vasca de Protección de Datos procederá recurso contencioso-administrativo. Podrá interponerse con carácter previo, potestativamente, recurso de reposición.

TÍTULO II

La Agencia Vasca de Protección de Datos

Artículo 10. *Creación y régimen jurídico.*

1. Se crea la Agencia Vasca de Protección de Datos como ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en esta ley y en su estatuto propio, que será aprobado por decreto del Gobierno Vasco a propuesta de la Vicepresidencia.
2. La Agencia Vasca de Protección de Datos sujetará su actividad a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuando ejerza potestades administrativas. En el resto de su actividad se someterá a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en esta ley y en las disposiciones de desarrollo de las mismas.
3. La Agencia Vasca de Protección de Datos estará sujeta al derecho público vigente en materia de adquisiciones patrimoniales y contratación. Sus bienes y derechos pertenecerán al patrimonio de la Comunidad Autónoma del País Vasco.
4. La representación y defensa en juicio de la Agencia Vasca de Protección de Datos estará a cargo de los servicios jurídicos de la Administración de la Comunidad Autónoma del País Vasco, conforme a lo dispuesto en sus normas reguladoras.

Artículo 11. *Personal.*

1. Los puestos de trabajo de la Agencia Vasca de Protección de Datos serán desempeñados por funcionarios de las administraciones públicas e instituciones a que se refiere el artículo 2.1 de esta ley y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal estará obligado a guardar secreto respecto a los datos de carácter personal que conozca en el desarrollo de su función.
2. El personal al servicio de la Agencia Vasca de Protección de Datos estará sometido a la normativa reguladora de la función pública en la Administración General de la Comunidad Autónoma. De conformidad con la misma, corresponde a la Agencia Vasca de Protección de Datos determinar el régimen de acceso a sus puestos de trabajo, los requisitos y las características de las pruebas de selección, así como la convocatoria, gestión y resolución de los procedimientos de provisión de puestos de trabajo y promoción profesional.

3. Los puestos de trabajo que comporten el ejercicio de potestades públicas estarán reservados a personal funcionario.

Artículo 12. *Recursos.*

La Agencia Vasca de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales de la Comunidad Autónoma.
b) Las subvenciones y aportaciones que se concedan a su favor.
c) Los ingresos, ordinarios y extraordinarios, derivados del ejercicio de sus actividades.
d) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
e) Cualesquiera otros que legalmente puedan serle atribuidos.

Artículo 13. *Presupuesto.*

La Agencia Vasca de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno Vasco para que sea integrado, con la debida independencia, en los Presupuestos Generales de la Comunidad Autónoma, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco. Estará sometida a esta legislación en lo relativo al régimen de modificación, ejecución y liquidación de su presupuesto, atendiendo a estos efectos a la naturaleza de la entidad; al régimen de contabilidad pública y al control económico financiero y de gestión del Departamento de Hacienda y Administración Pública de la Administración de la Comunidad Autónoma, sin perjuicio de la fiscalización de sus actividades económico-financieras y contables por el Tribunal Vasco de Cuentas Públicas.

Artículo 14. *Órganos de gobierno.*

Son órganos de gobierno de la Agencia Vasca de Protección de Datos el director, el Consejo Consultivo y aquellos otros que se establezcan en su estatuto propio.

Artículo 15. *El director.*

1. El director de la Agencia Vasca de Protección de Datos dirige la agencia y ostenta su representación. Será nombrado por decreto del Gobierno Vasco, por un periodo de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquellas. No obstante, el director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.
3. El director de la Agencia Vasca de Protección de Datos sólo cesará antes de la expiración de su periodo por alguna de las siguientes causas:

a) A petición propia.
b) Por separación, acordada por el Consejo de Gobierno, previa instrucción de expediente, en el que necesariamente será oído el Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El director de la Agencia Vasca de Protección de Datos tendrá la consideración de alto cargo, quedará en la situación de servicios especiales si anteriormente estuviera desempeñando una función pública, y estará sometido al régimen de incompatibilidades de los altos cargos de la Administración de la Comunidad Autónoma.

Artículo 16. *El Consejo Consultivo.*

1. El director de la Agencia Vasca de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un representante del Parlamento Vasco, designado por éste.

b) Un representante de la Administración de la Comunidad Autónoma del País Vasco, designado por el Consejo de Gobierno.

c) Un representante de los territorios históricos, designado por éstos de común acuerdo.

d) Un representante de las entidades locales del ámbito territorial de la Comunidad Autónoma del País Vasco, designado por la asociación más representativa de las mismas en el citado ámbito territorial.

e) Dos expertos, uno en informática y otro en el ámbito de los derechos fundamentales, designados por la Universidad del País Vasco previa consulta a las corporaciones de derecho público de la Comunidad Autónoma del País Vasco.

2. El Consejo Consultivo aprobará sus propias normas de organización y funcionamiento, en las que se preverán las figuras de presidente y secretario, así como el sistema para su elección o designación.

Artículo 17. *Funciones.*

1. Son funciones de la Agencia Vasca de Protección de Datos, en relación con los ficheros a que se refiere el artículo 2.1 de esta ley y en el ámbito de las competencias de la Comunidad Autónoma del País Vasco:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en las leyes y reglamentos.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la legislación vigente en materia de protección de datos.

d) Atender las peticiones y reclamaciones formuladas por los afectados.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y a los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajuste a dicha legislación, salvo en la que se refiera a transferencias internacionales de datos.

g) Ejercer la potestad sancionadora y, en su caso, proponer la iniciación de procedimientos disciplinarios contra quienes estime responsables de las infracciones tipificadas en el artículo 22 de esta ley, así como adoptar las medidas cautelares que procedan, salvo en lo que se refiera a las transferencias internacionales de datos. Todo ello en los términos previstos en esta ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará anualmente una relación de dichos ficheros con la información adicional que el director de la Agencia Vasca de Protección de Datos determine.

k) Redactar una memoria anual y remitirla a la Vicepresidencia del Gobierno Vasco.

l) Velar por el cumplimiento de las disposiciones que la legislación sobre la función estadística pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 24.

m) Colaborar con la Agencia de Protección de Datos del Estado y entidades similares de otras comunidades autónomas en cuantas actividades sean necesarias para una mejor protección de la seguridad de los ficheros de datos de carácter personal y de los derechos de los ciudadanos en relación con los mismos.

n) Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta ley.

ñ) Cuantas otras le sean atribuidas por las leyes y reglamentos.

2. A los efectos de las funciones a que se refiere el número anterior, la Agencia Vasca de Protección de Datos tendrá la consideración de autoridad de control, y la ley le garantiza la plena independencia y objetividad en el ejercicio de su cometido.

Artículo 18. *Registro de Protección de Datos.*

1. Se crea el Registro de Protección de Datos, como órgano integrado en la Agencia Vasca de Protección de Datos en los términos que se establezcan en los estatutos de ésta.

2. Serán objeto de inscripción en el Registro de Protección de Datos:

a) Los ficheros a los que se refiere el artículo 2.1 de esta ley.

b) Las autorizaciones a las que se refiere la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

c) Los códigos tipo que afecten a los ficheros inscritos.

d) Los datos relativos a los ficheros inscritos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. El Registro de Protección de Datos podrá denegar la inscripción solicitada cuando considere que la petición no se ajusta a derecho. En este caso, el director de la Agencia Vasca de Protección de Datos deberá requerir al solicitante para que efectúe las correcciones oportunas.

4. Reglamentariamente se regulará el procedimiento de inscripción de los ficheros a los que se refiere el artículo 2.1 de esta ley en el Registro de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes, y demás extremos pertinentes.

5. El Registro de Protección de Datos será de consulta pública y gratuita. Cualquier persona podrá conocer, recabando la información oportuna del citado registro, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

Artículo 19. *Potestad de inspección.*

1. La Agencia Vasca de Protección de Datos, como autoridad de control, podrá inspeccionar los ficheros a los que se refiere el artículo 2.1 de esta ley, recabando cuanta información precise para el cumplimiento de su cometido. A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el número anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos, y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de sus funciones, incluso después de haber cesado en las mismas.

Artículo 20. *Requerimientos a los titulares de los ficheros.*

Cuando el director de la Agencia Vasca de Protección de Datos constate que el mantenimiento y uso de un determinado fichero incluido en el ámbito de aplicación de esta ley contraviene algún precepto de la misma o de las disposiciones que la desarrollen, podrá requerir a la administración pública, institución o corporación titular del fichero que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento. Si la administración requerida incumpliera el requerimiento formulado, el director de la Agencia Vasca de Protección de Datos, sin perjuicio de otras medidas que pueda adoptar de acuerdo con el artículo 17.f) de esta ley, podrá recurrir la resolución o la actitud omisiva adoptada por aquella administración, teniendo, a estos efectos, la condición de interesado.

TÍTULO III

Régimen sancionador

Artículo 21. *Responsables.*

Los responsables de los ficheros a los que se refiere el artículo 2.1 de esta ley y los encargados de los tratamientos de los mismos estarán sujetos al régimen de infracciones y sanciones establecido en esta ley.

Artículo 22. *Tipos de infracciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.
2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento, cuando legalmente proceda.
b) No proporcionar la información que solicite la Agencia Vasca de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro de Protección de Datos, cuando no sea constitutivo de infracción grave.
d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información legalmente exigida.
e) Incumplir el deber de secreto legalmente establecido, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros, o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general publicada en el «Boletín Oficial del País Vasco» o en el del territorio histórico correspondiente.
b) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigido.
c) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías legalmente establecidos o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
d) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
e) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente proceda cuando resulten afectados los derechos de las personas amparadas por la legislación de protección de datos de carácter personal.
f) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales o a Hacienda pública, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
g) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.
h) No remitir a la Agencia Vasca de Protección de Datos las comunicaciones previstas en las leyes y reglamentos, así como no proporcionar a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquélla a tales efectos.
i) La obstrucción al ejercicio de la función inspectora.
j) No inscribir el fichero de datos de carácter personal en el Registro de Protección de Datos, cuando haya sido requerido para ello por el director de la Agencia Vasca de Protección de Datos.
k) Incumplir el deber de información legalmente establecido, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.
b) La comunicación o cesión de datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recabar y tratar datos de carácter personal que revelen ideología, afiliación sindical, religión o creencias, cuando no medie consentimiento expreso del afectado.
d) Recabar y tratar datos referidos al origen racial, a la salud o a la vida sexual, cuando no lo disponga una ley o el afectado no haya consentido expresamente.
e) Crear ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual.
f) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el director de la Agencia Vasca de Protección de Datos o por los titulares del derecho de acceso.
g) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
h) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hace referencia la letra e) de este mismo apartado, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
i) No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
j) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

5. La tipificación de infracciones que contiene este artículo se entiende sin perjuicio de las tipificadas en la legislación estatal sobre protección de datos, en aquellos aspectos sobre los que la Comunidad Autónoma del País Vasco carece de competencia.

Artículo 23. *Tipos de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 601,01 a 60.101,21 euros.
2. Las infracciones graves serán sancionadas con multa de 60.101,21 a 300.506,05 euros.
3. Las infracciones muy graves serán sancionadas con multa de 300.506,05 a 601.012,1 euros.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquélla en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno Vasco actualizará periódicamente la cuantía de las sanciones, de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 24. *Infracciones cometidas por las administraciones públicas, instituciones y corporaciones de Derecho público.*

1. Cuando, instruido el correspondiente procedimiento, se llegue a la conclusión de que se ha cometido alguna o algunas de las infracciones a que se refiere el artículo anterior, en relación con los ficheros a que se refiere el artículo 2.1 de esta ley, el director de la Agencia Vasca de Protección de Datos dictará una resolución estableciendo las medidas que

procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera, y la misma agota la vía administrativa.

2. El director de la Agencia Vasca de Protección de Datos podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán los establecidos en la legislación reguladora del régimen disciplinario de los funcionarios y personal al servicio de las administraciones públicas, instituciones y corporaciones a las que se refiere el artículo 2.1 de esta ley. A estos efectos, las infracciones tipificadas en esta ley completarán el régimen disciplinario que sea de aplicación.

3. En el supuesto de que haya que seguir un procedimiento sancionador, se estará a lo dispuesto en la Ley 2/1998, de 20 de febrero, de la Potestad Sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco.

4. Se deberán comunicar a la Agencia Vasca de Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los números anteriores.

5. El director de la Agencia Vasca de Protección de Datos comunicará al Ararteko las actuaciones que efectúe y las resoluciones que dicte al amparo de los números anteriores.

Artículo 25. *Inmovilización de ficheros.*

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el director de la Agencia Vasca de Protección de Datos podrá requerir a los responsables de ficheros de datos de carácter personal la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Comunicación de ficheros a la Agencia Vasca de Protección de Datos.*

Las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1) de esta ley comunicarán a la Agencia Vasca de Protección de Datos, en el plazo de tres meses a partir de la entrada en vigor de esta ley, los ficheros de datos de carácter personal señalados en aquel precepto que sean de su titularidad. Previamente deberán tener aprobada y publicada la disposición reguladora del correspondiente fichero.

Disposición adicional segunda. *Comunicación de datos del padrón.*

1. Las administraciones general y forales de la Comunidad Autónoma del País Vasco podrán solicitar al Euskal Estatistika-Erakundea/Instituto Vasco de Estadística, en los términos que se establecen en la disposición adicional segunda de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y artículo 17.3 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. Estos ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas de las administraciones públicas.

2. A los efectos de lo dispuesto en el párrafo anterior, se modifica el artículo 29 de la Ley 4/1986, de 28 de abril, de Estadística de la Comunidad Autónoma de Euskadi, en los siguientes términos: la redacción actual del citado precepto queda como número 1 del mismo, al que se añade un número 2 con el siguiente texto:

> «2. El Euskal Estatistika-Erakundea/Instituto Vasco de Estadística actuará también como depositario de copias de los padrones municipales de todos los municipios de la Comunidad Autónoma del País Vasco, a cuyos efectos éstos le

deberán remitir copias de los citados registros administrativos en los términos que se establezcan reglamentariamente.»

Disposición adicional tercera. *Competencias del Ararteko y de la Agencia de Protección de Datos del Estado.*

Lo dispuesto en esta ley se entiende sin perjuicio de las competencias que tengan atribuidas el Ararteko y la Agencia de Protección de Datos del Estado.

Disposición final. *Desarrollo y aplicación.*

1. Se autoriza al Gobierno Vasco para el desarrollo y aplicación de lo dispuesto en esta ley.

2. Se autoriza al Departamento de Hacienda y Administración Pública para crear la sección presupuestaria correspondiente y para realizar, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco, las modificaciones presupuestarias precisas para la aplicación de lo dispuesto en esta ley.

§ 12

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Jefatura del Estado
«BOE» núm. 166, de 12 de julio de 2002
Última modificación: 12 de noviembre de 2020
Referencia: BOE-A-2002-13758

JUAN CARLOS I REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

La presente Ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

Lo que la Directiva 2000/31/CE denomina "sociedad de la información" viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.

Pero la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio.

Eso es lo que pretende esta Ley, que parte de la aplicación a las actividades realizadas por medios electrónicos de las normas tanto generales como especiales que las regulan, ocupándose tan sólo de aquellos aspectos que, ya sea por su novedad o por las

peculiaridades que implica su ejercicio por vía electrónica, no están cubiertos por dicha regulación.

II

Se acoge, en la Ley, un concepto amplio de "servicios de la sociedad de la información", que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Desde un punto de vista subjetivo, la Ley se aplica, con carácter general, a los prestadores de servicios establecidos en España. Por "establecimiento" se entiende el lugar desde el que se dirige y gestiona una actividad económica, definición esta que se inspira en el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada por el Derecho comunitario. La Ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de la información a través de un "establecimiento permanente" situado en España. En este último caso, la sujeción a la Ley es únicamente parcial, respecto a aquellos servicios que se presten desde España.

El lugar de establecimiento del prestador de servicios es un elemento esencial en la Ley, porque de él depende el ámbito de aplicación no sólo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean de aplicación, en función de la actividad que desarrollen. Asimismo, el lugar de establecimiento del prestador determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de la aplicación de la ley del país de origen que inspira la Directiva 2000/31/CE.

Por lo demás, sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países pertenecientes al Espacio Económico Europeo en los supuestos previstos en la Directiva 2000/31/CE, que consisten en la producción de un daño o peligro graves contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores. Igualmente, podrá restringirse la prestación de servicios provenientes de dichos Estados cuando afecten a alguna de las materias excluidas del principio de país de origen, que la Ley concreta en su artículo 3, y se incumplan las disposiciones de la normativa española que, en su caso, resulte aplicable a las mismas.

III

Se prevé la anotación del nombre o nombres de dominio de Internet que correspondan al prestador de servicios en el registro público en que, en su caso, dicho prestador conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con el fin de garantizar que la vinculación entre el prestador, su establecimiento físico y su "establecimiento" o localización en la red, que proporciona su dirección de Internet, sea fácilmente accesible para los ciudadanos y la Administración pública.

La Ley establece, asimismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que pueden derivar del incumplimiento de

estas normas no son sólo de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables.

Destaca, por otra parte, en la Ley, su afán por proteger los intereses de los destinatarios de servicios, de forma que éstos puedan gozar de garantías suficientes a la hora de contratar un servicio o bien por Internet. Con esta finalidad, la Ley impone a los prestadores de servicios la obligación de facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en Internet; la de informar a los destinatarios sobre los precios que apliquen a sus servicios y la de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se someta, en su caso, el contrato. Cuando la contratación se efectúe con consumidores, el prestador de servicios deberá, además, guiarles durante el proceso de contratación, indicándoles los pasos que han de dar y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida.

En lo que se refiere a las comunicaciones comerciales, la Ley establece que éstas deban identificarse como tales, y prohíbe su envío por correo electrónico u otras vías de comunicación electrónica equivalente, salvo que el destinatario haya prestado su consentimiento.

IV

Se favorece igualmente la celebración de contratos por vía electrónica, al afirmar la Ley, de acuerdo con el principio espiritualista que rige la perfección de los contratos en nuestro Derecho, la validez y eficacia del consentimiento prestado por vía electrónica, declarar que no es necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes, y asegurar la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de "forma escrita" que figura en diversas leyes.

Se aprovecha la ocasión para fijar el momento y lugar de celebración de los contratos electrónicos, adoptando una solución única, también válida para otros tipos de contratos celebrados a distancia, que unifica el criterio dispar contenido hasta ahora en los Códigos Civil y de Comercio.

Las disposiciones contenidas en esta Ley sobre aspectos generales de la contratación electrónica, como las relativas a la validez y eficacia de los contratos electrónicos o al momento de prestación del consentimiento, serán de aplicación aun cuando ninguna de las partes tenga la condición de prestador o destinatario de servicios de la sociedad de la información.

La Ley promueve la elaboración de códigos de conducta sobre las materias reguladas en esta Ley, al considerar que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la Ley a las características específicas de cada sector.

Por su sencillez, rapidez y comodidad para los usuarios, se potencia igualmente el recurso al arbitraje y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta, para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información. Se favorece, además, el uso de medios electrónicos en la tramitación de dichos procedimientos, respetando, en su caso, las normas que, sobre la utilización de dichos medios, establezca la normativa específica sobre arbitraje.

De conformidad con lo dispuesto en las Directivas 2000/31/CE y 98/27/CE, se regula la acción de cesación que podrá ejercitarse para hacer cesar la realización de conductas contrarias a la presente Ley que vulneren los intereses de los consumidores y usuarios. Para el ejercicio de esta acción, deberá tenerse en cuenta, además de lo dispuesto en esta Ley, lo establecido en la Ley general de incorporación de la Directiva 98/27/CE.

La Ley prevé, asimismo, la posibilidad de que los ciudadanos y entidades se dirijan a diferentes Ministerios y órganos administrativos para obtener información práctica sobre distintos aspectos relacionados con las materias objeto de esta Ley, lo que requerirá el establecimiento de mecanismos que aseguren la máxima coordinación entre ellos y la homogeneidad y coherencia de la información suministrada a los usuarios.

Finalmente, se establece un régimen sancionador proporcionado pero eficaz, como indica la Directiva 2000/31/CE, para disuadir a los prestadores de servicios del incumplimiento de lo dispuesto en esta Ley.

Asimismo, se contempla en la Ley una serie de previsiones orientadas a hacer efectiva la accesibilidad de las personas con discapacidad a la información proporcionada por medios electrónicos, y muy especialmente a la información suministrada por las Administraciones públicas, compromiso al que se refiere la resolución del Consejo de la Unión Europea de 25 de marzo de 2002, sobre accesibilidad de los sitios web públicos y de su contenido.

La presente disposición ha sido elaborada siguiendo un amplio proceso de consulta pública y ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio, y en el Real Decreto 1337/1999, de 31 de julio.

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto

Artículo 1. *Objeto.*

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.

CAPÍTULO II

Ámbito de aplicación

Artículo 2. *Prestadores de servicios establecidos en España.*

1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

Artículo 3. *Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.*

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

a) Derechos de propiedad intelectual o industrial.

b) Emisión de publicidad por instituciones de inversión colectiva.

c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.

d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.

e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.

f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Artículo 4. *Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo.*

A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo, les será de aplicación lo dispuesto en los artículos 7.2 y 11.2.

Los prestadores que dirijan sus servicios específicamente al territorio español quedarán sujetos, además, a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables.

Artículo 5. *Servicios excluidos del ámbito de aplicación de la Ley.*

1. Se regirán por su normativa específica las siguientes actividades y servicios de la sociedad de la información:

a) Los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas.

b) Los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

2. Las disposiciones de la presente Ley, con la excepción de lo establecido en el artículo 7.1, serán aplicables a los servicios de la sociedad de la información relativos a juegos de

azar que impliquen apuestas de valor económico, sin perjuicio de lo establecido en su legislación específica estatal o autonómica.

TÍTULO II

Prestación de servicios de la sociedad de la información

CAPÍTULO I

Principio de libre prestación de servicios

Artículo 6. *No sujeción a autorización previa.*

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa.

Esta norma no afectará a los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios.

Artículo 7. *Principio de libre prestación de servicios.*

1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo se realizará en régimen de libre prestación de servicios, sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8.

2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atendrá a los acuerdos internacionales que resulten de aplicación.

Artículo 8. *Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.*

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

e) La salvaguarda de los derechos de propiedad intelectual.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

2. Los órganos competentes para la adopción de las medidas a que se refiere el apartado anterior, con el objeto de identificar al responsable del servicio de la sociedad de la información que está realizando la conducta presuntamente vulneradora, podrán requerir a los prestadores de servicios de la sociedad de la información la cesión de los datos que permitan tal identificación a fin de que pueda comparecer en el procedimiento. Tal requerimiento exigirá la previa autorización judicial de acuerdo con lo previsto en el apartado primero del artículo 122 bis de la Ley reguladora de la Jurisdicción contencioso-administrativa. Una vez obtenida la autorización, los prestadores estarán obligados a facilitar los datos necesarios para llevar a cabo la identificación.

3. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

4. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

5. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

6. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.

CAPÍTULO II

Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información

Sección 1.ª Obligaciones

Artículo 9. *Constancia registral del nombre de dominio.*

(Sin contenido)

Artículo 10. *Información general.*

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los

órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

Artículo 11. *Deber de colaboración de los prestadores de servicios de intermediación.*

1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados

prestadores que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

Artículo 12. *Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.*

(Derogado)

Artículo 12 bis. *Obligaciones de información sobre seguridad.*

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.

Artículo 12 ter. *Obligaciones relativas a la portabilidad de datos no personales.*

Los proveedores de servicios de intermediación que alojen o almacenen datos de usuarios a los que presten servicios de redes sociales o servicios de la sociedad de la información equivalentes deberán remitir a dichos usuarios, a su solicitud, los contenidos que les hubieran facilitado, sin impedir su transmisión posterior a otro proveedor. La remisión deberá efectuarse en un formato estructurado, de uso común y lectura mecánica.

Asimismo, deberán transmitir dichos contenidos directamente a otro proveedor designado por el usuario, siempre que sea técnicamente posible, según prevé el artículo 95 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Para el cumplimiento de estas obligaciones será aplicable lo dispuesto en el artículo 12.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Sección 2.ª Régimen de responsabilidad

Artículo 13. *Responsabilidad de los prestadores de los servicios de la sociedad de la información.*

1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.

Artículo 14. *Responsabilidad de los operadores de redes y proveedores de acceso.*

1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.

2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

Artículo 15. *Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.*

Los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

a) No modifican la información.

b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y e) Retiran la

información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.
2.º Que se ha imposibilitado el acceso a ella, o 3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

Artículo 16. *Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.*

1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.

Artículo 17. *Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.*

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

CAPÍTULO III

Códigos de conducta

Artículo 18. *Códigos de conducta.*

1. Las administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta que afecten a los consumidores y usuarios estarán sujetos, además, al capítulo V de la Ley 3/1991, de 10 de enero, de competencia desleal.

Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.

2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias.

Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.

3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.

TÍTULO III

Comunicaciones comerciales por vía electrónica

Artículo 19. *Régimen jurídico.*

1. Las comunicaciones comerciales y las ofertas promocionales se regirán, además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad.

2. En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Artículo 20. *Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo.

4. En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo.

Artículo 21. *Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Artículo 22. *Derechos de los destinatarios de servicios.*

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

TÍTULO IV

Contratación por vía electrónica

Artículo 23. *Validez y eficacia de los contratos celebrados por vía electrónica.*

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.

Artículo 24. *Prueba de los contratos celebrados por vía electrónica.*

1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

Artículo 25. *Intervención de terceros de confianza.*

(Derogado)

Artículo 26. *Ley aplicable.*

Para la determinación de la ley aplicable a los contratos electrónicos se estará a lo dispuesto en las normas de Derecho internacional privado del ordenamiento jurídico español, debiendo tomarse en consideración para su aplicación lo establecido en los artículos 2 y 3 de esta Ley.

Artículo 27. *Obligaciones previas a la contratación.*

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.

b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.

c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y

d) La lengua o lenguas en que podrá formalizarse el contrato.

La obligación de poner a disposición del destinatario la información referida en el párrafo anterior se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en dicho párrafo.

Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.

3. Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.

4. Con carácter previo al inicio del procedimiento de contratación, el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Artículo 28. *Información posterior a la celebración del contrato.*

1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

a) El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o

b) La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.

2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.

En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.

Artículo 29. *Lugar de celebración del contrato.*

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.

Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

TÍTULO V

Solución judicial y extrajudicial de conflictos

CAPÍTULO I

Acción de cesación

Artículo 30. *Acción de cesación.*

1. Contra las conductas contrarias a la presente Ley que lesionen intereses colectivos o difusos de los consumidores podrá interponerse acción de cesación.
2. La acción de cesación se dirige a obtener una sentencia que condene al demandado a cesar en la conducta contraria a la presente Ley y a prohibir su reiteración futura. Asimismo, la acción podrá ejercerse para prohibir la realización de una conducta cuando ésta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inminente.
3. La acción de cesación se ejercerá conforme a las prescripciones de la Ley de Enjuiciamiento Civil para esta clase de acciones.

Artículo 31. *Legitimación activa.*

Están legitimados para interponer la acción de cesación:

a) Las personas físicas o jurídicas titulares de un derecho o interés legítimo, incluidas aquéllas que pudieran verse perjudicadas por infracciones de las disposiciones contenidas en los artículos 21 y 22, entre ellas, los proveedores de servicios de comunicaciones electrónicas que deseen proteger sus intereses comerciales legítimos o los intereses de sus clientes.
b) Los grupos de consumidores o usuarios afectados, en los casos y condiciones previstos en la Ley de Enjuiciamiento Civil.
c) Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, o, en su caso, en la legislación autonómica en materia de defensa de los consumidores.
d) El Ministerio Fiscal.
e) El Instituto Nacional del Consumo y los órganos correspondientes de las Comunidades Autónomas y de las Corporaciones Locales competentes en materia de defensa de los consumidores.
f) Las entidades de otros Estados miembros de la Unión Europea constituidas para la protección de los intereses colectivos o difusos de los consumidores que estén habilitadas ante la Comisión Europea mediante su inclusión en la lista publicada a tal fin en el "Diario Oficial de las Comunidades Europeas".
Los Jueces y Tribunales aceptarán dicha lista como prueba de la capacidad de la entidad habilitada para ser parte, sin perjuicio de examinar si la finalidad de la misma y los intereses afectados legitiman el ejercicio de la acción.

CAPÍTULO II

Solución extrajudicial de conflictos

Artículo 32. *Solución extrajudicial de conflictos.*

1. El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos a los arbitrajes previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios, y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación.

2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos, en los términos que establezca su normativa específica.

TÍTULO VI

Información y control

Artículo 33. *Información a los destinatarios y prestadores de servicios.*

Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de sociedad de la información, sanidad y consumo de las Administraciones Públicas, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica,

b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y

c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.

Artículo 34. *Comunicación de resoluciones relevantes.*

1. El Consejo General del Poder Judicial remitirá al Ministerio de Justicia, en la forma y con la periodicidad que se acuerde mediante Convenio entre ambos órganos, todas las resoluciones judiciales que contengan pronunciamientos relevantes sobre la validez y eficacia de los contratos celebrados por vía electrónica, sobre su utilización como prueba en juicio, o sobre los derechos, obligaciones y régimen de responsabilidad de los destinatarios y los prestadores de servicios de la sociedad de la información.

2. Los órganos arbitrales y los responsables de los demás procedimientos de resolución extrajudicial de conflictos a que se refiere el artículo 32.1 comunicarán al Ministerio de Justicia los laudos o decisiones que revistan importancia para la prestación de servicios de la sociedad de la información y el comercio electrónico de acuerdo con los criterios indicados en el apartado anterior.

3. En la comunicación de las resoluciones, laudos y decisiones a que se refiere este artículo, se tomarán las precauciones necesarias para salvaguardar el derecho a la intimidad y a la protección de los datos personales de las personas identificadas en ellos.

4. El Ministerio de Justicia remitirá a la Comisión Europea y facilitará el acceso de cualquier interesado a la información recibida de conformidad con este artículo.

Artículo 35. *Supervisión y control.*

1. El Ministerio de Asuntos Económicos y Transformación Digital controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información, así como en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, por parte de aquellos proveedores incluidos en su ámbito de aplicación.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. Los órganos citados en el apartado 1 de este artículo podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos a dichos órganos y que ejerzan la inspección a que se refiere el párrafo anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. En todo caso, y no obstante lo dispuesto en el apartado anterior, cuando las conductas realizadas por los prestadores de servicios de la sociedad de la información estuvieran sujetas, por razón de la materia o del tipo de entidad de que se trate, a ámbitos competenciales, de tutela o de supervisión específicos, con independencia de que se lleven a cabo utilizando técnicas y medios telemáticos o electrónicos, los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica ejercerán las funciones que les correspondan.

Artículo 36. *Deber de colaboración.*

1. Los prestadores de servicios de la sociedad de la información tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología y a los demás órganos a que se refiere el artículo anterior toda la información y colaboración precisas para el ejercicio de sus funciones.

Igualmente, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

2. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, estatales o autonómicas, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 36 bis. *Deber de comunicación de las organizaciones y asociaciones representativas de usuarios profesionales o de los usuarios de sitios web corporativos.*

Las organizaciones y asociaciones que posean un interés legítimo de representación de usuarios profesionales o de los usuarios de sitios web corporativos, y que, cumpliendo con los requisitos del artículo 14.3 del Reglamento (UE) 2019/1150, hubieren solicitado al Ministerio de Asuntos Económicos y Transformación Digital su inclusión en la lista elaborada al efecto por la Comisión Europea, notificarán inmediatamente al citado Ministerio cualquier circunstancia que afecte a su entidad que derive en un incumplimiento sobrevenido de los mencionados requisitos.

TÍTULO VII

Infracciones y sanciones

Artículo 37. *Responsables.*

Los prestadores de servicios de la sociedad de la información a los que les sea de aplicación la presente Ley, así como los proveedores incluidos en el ámbito de aplicación del Reglamento (UE) 2019/1150, están sujetos al régimen sancionador establecido en este Título.

Cuando las infracciones previstas en el artículo 38.3 i) y 38.4 g) se deban a la instalación de dispositivos de almacenamiento y recuperación de la información como consecuencia de la cesión por parte del prestador del servicio de la sociedad de la información de espacios propios para mostrar publicidad, será responsable de la infracción, además del prestador del servicio de la sociedad de la información, la red publicitaria o agente que gestione directamente con aquel la colocación de anuncios en dichos espacios en caso de no haber adoptado medidas para exigirle el cumplimiento de los deberes de información y la obtención del consentimiento del usuario.

Artículo 38. *Infracciones.*

1. Las infracciones de los preceptos de esta Ley se calificarán como muy graves, graves y leves.

2. Son infracciones muy graves:

a) **(Sin contenido)**

b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

c) **(Derogado)**

d) **(Derogado)**

3. Son infracciones graves:

a) **(Derogado)**

b) El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.

c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.

d) El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.

e) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.

f) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

g) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley.

h) El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.

i) La reincidencia en la comisión de la infracción leve prevista en el apartado 4 g) cuando así se hubiera declarado por resolución firme dictada en los tres años inmediatamente anteriores a la apertura del procedimiento sancionador.

j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, fuera de los supuestos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679.

k) El incumplimiento habitual de la obligación prevista en el artículo 12 ter.

l) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional.

m) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150.

n) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables.

o) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos.

p) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios.

q) El incumplimiento por parte de los proveedores de servicios de intermediación de la obligación establecida en la letra a) del artículo 8 del Reglamento (UE) 2019/1150, así como el incumplimiento habitual de las obligaciones contenidas en las letras b) y c) del citado precepto.

r) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150.

s) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150.

t) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de establecer un sistema interno y gratuito para tramitar las reclamaciones de los usuarios profesionales, en los términos previstos por el artículo 11 del Reglamento (UE) 2019/1150.

u) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de designar al menos dos mediadores, o de cualquier otra de las obligaciones en materia de mediación establecidas en el artículo 12 del Reglamento (UE) 2019/1150.

4. Son infracciones leves:

a) El incumplimiento de lo previsto en el art. 12 bis.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

g) Utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2.

h) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

i) El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave.

j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, cuando así lo permita el artículo 12.5 del Reglamento (UE) 2016/679, si su cuantía excediese el importe de los costes afrontados.

k) El incumplimiento de la obligación prevista en el artículo 12 ter, cuando no constituya infracción grave.

l) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional, cuando no constituya infracción grave.

m) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

n) El incumplimiento por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables, cuando no constituya infracción grave.

o) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos, cuando no constituya infracción grave.

p) El incumplimiento por parte de los proveedores de servicios de intermediación en línea y los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios, cuando no constituya infracción grave.

q) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de las obligaciones en materia de cláusulas contractuales específicas establecidas en el artículo 8 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

r) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

s) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

Artículo 39. *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el "Boletín Oficial del Estado", o en el diario oficial de la Administración pública que, en su caso, hubiera impuesto la sanción; en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada Administración pública o en la página de inicio del sitio de Internet del prestador, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, por el número de usuarios o de contratos afectados, y la gravedad del ilícito.

3. Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves.

Artículo 39 bis. *Moderación de sanciones.*

1. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 40.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el órgano competente no hubiese sancionado o apercibido con anterioridad al infractor como consecuencia de la comisión de infracciones previstas en esta Ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 40. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:

a) La existencia de intencionalidad.

b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.

c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.

d) La naturaleza y cuantía de los perjuicios causados.

e) Los beneficios obtenidos por la infracción.

f) Volumen de facturación a que afecte la infracción cometida.

g) La adhesión a un código de conducta o a un sistema de autorregulación publicitaria aplicable respecto a la infracción cometida, que cumpla con lo dispuesto en el artículo 18 o en la disposición final octava y que haya sido informado favorablemente por el órgano u órganos competentes.

Artículo 41. *Medidas de carácter provisional.*

1. En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c) Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan

competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en el presente artículo podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 42. *Multa coercitiva.*

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 43. *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren las letras a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.

Artículo 44. *Concurrencia de infracciones y sanciones.*

1. No podrá ejercerse la potestad sancionadora a que se refiere la presente Ley cuando haya recaído sanción penal, en los casos en que se aprecie identidad de sujeto, hecho y fundamento.

No obstante, cuando se esté tramitando un proceso penal por los mismos hechos o por otros cuya separación de los sancionables con arreglo a esta Ley sea racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta que recaiga pronunciamiento firme de la autoridad judicial.

Reanudado el expediente, en su caso, la resolución que se dicte deberá respetar los hechos declarados probados en la resolución judicial.

2. La imposición de una sanción prevista en esta Ley no impedirá la tramitación y resolución de otro procedimiento sancionador por los órganos u organismos competentes en cada caso cuando la conducta infractora se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3. No procederá la imposición de sanciones según lo previsto en esta Ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará

cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 45. *Prescripción.*

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

Disposición adicional primera. *Significado de los términos empleados por esta Ley.*

A los efectos de la presente Ley, los términos definidos en el anexo tendrán el significado que allí se les asigna.

Disposición adicional segunda. *Medicamentos y productos sanitarios.*

La prestación de servicios de la sociedad de la información relacionados con los medicamentos y los productos sanitarios se regirá por lo dispuesto en su legislación específica.

Disposición adicional tercera. *Sistema Arbitral de Consumo.*

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente que se prestará también por medios electrónicos, conforme al procedimiento establecido reglamentariamente.

Disposición adicional cuarta. *Modificación de los Códigos Civil y de Comercio.*

Uno. Se modifica el artículo 1.262 del Código Civil, que queda redactado de la siguiente manera:

> «El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.
>
> Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.
>
> En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Dos. Se modifica el artículo 54 del Código de Comercio, que queda redactado de la siguiente manera:

> «Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.
>
> En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Disposición adicional quinta. *Accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos.*

Uno. Las Administraciones públicas adoptarán las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005.

A partir del 31 de diciembre de 2008, las páginas de Internet de las Administraciones Públicas satisfarán, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

Las Administraciones Públicas exigirán que tanto las páginas de Internet cuyo diseño o mantenimiento financien total o parcialmente como las páginas de Internet de entidades y empresas que se encarguen de gestionar servicios públicos apliquen los criterios de accesibilidad antes mencionados. En particular, será obligatorio lo expresado en este apartado para las páginas de Internet y sus contenidos de los Centros públicos educativos, de formación y universitarios, así como, de los Centros privados que obtengan financiación pública.

Las páginas de Internet de las Administraciones Públicas deberán ofrecer al usuario información sobre su nivel de accesibilidad y facilitar un sistema de contacto para que puedan transmitir las dificultades de acceso al contenido de las páginas de Internet o formular cualquier queja, consulta o sugerencia de mejora.

Dos. Igualmente, se promoverá la adopción de normas de accesibilidad por los prestadores de servicios y los fabricantes de equipos y "software", para facilitar el acceso de las personas con discapacidad o de edad avanzada a los contenidos digitales.

Tres. Las Administraciones Públicas promoverán medidas de sensibilización, educación y formación sobre accesibilidad con objeto de promover que los titulares de otras páginas de Internet incorporen progresivamente los criterios de accesibilidad.

Cuatro. Los incumplimientos de las obligaciones de accesibilidad establecidas en esta Disposición adicional estarán sometidos al régimen de infracciones y sanciones vigente en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Cinco. Las páginas de Internet de las empresas que presten servicios al público en general de especial trascendencia económica, sometidas a la obligación establecida en el artículo 2 de la Ley 56/2007, de medidas de impulso de la sociedad de la información, deberán satisfacer a partir del 31 de diciembre de 2008, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

Seis. Las páginas de Internet que sirvan de soporte o canal a las redes sociales en línea, desarrolladas por entidades cuyo volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.101.121,04 euros, deberán satisfacer, a partir del 31 de diciembre de 2012, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad

Disposición adicional sexta. *Sistema de asignación de nombres de dominio bajo el ".es".*

Uno. Esta disposición regula, en cumplimiento de lo previsto en la disposición adicional decimosexta de la Ley 17/2001, de 7 de diciembre, de Marcas, los principios inspiradores del sistema de asignación de nombres de dominio bajo el código de país correspondiente a España ".es".

Dos. La entidad pública empresarial Red.es es la autoridad de asignación, a la que corresponde la gestión del registro de nombres de dominio de Internet bajo el ".es", de acuerdo con lo establecido en la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

Tres. La asignación de nombres de dominio de Internet bajo el ".es" se realizará de conformidad con los criterios que se establecen en esta disposición, en el Plan Nacional de Nombres de Dominio de Internet, en las demás normas específicas que se dicten en su desarrollo por la autoridad de asignación y, en la medida en que sean compatibles con ellos, con las prácticas generalmente aplicadas y las recomendaciones emanadas de las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión del sistema de nombres de dominio de Internet.

Los criterios de asignación de nombres de dominio bajo el ".es" deberán garantizar un equilibrio adecuado entre la confianza y seguridad jurídica precisas para el desarrollo del comercio electrónico y de otros servicios y actividades por vía electrónica, y la flexibilidad y agilidad requeridas para posibilitar la satisfacción de la demanda de asignación de nombres

de dominio bajo el ".es", contribuyendo, de esta manera, al desarrollo de la sociedad de la información en España.

Podrán crearse espacios diferenciados bajo el ".es", que faciliten la identificación de los contenidos que alberguen en función de su titular o del tipo de actividad que realicen. Entre otros, podrán crearse indicativos relacionados con la educación, el entretenimiento y el adecuado desarrollo moral de la infancia y juventud. Estos nombres de dominio de tercer nivel se asignarán en los términos que se establezcan en el Plan Nacional de Nombres de Dominio de Internet.

Cuatro. Podrán solicitar la asignación de nombres de dominio bajo el ".es", en los términos que se prevean en el Plan Nacional de Nombres de Dominio de Internet, todas las personas o entidades, con o sin personalidad jurídica, que tengan intereses o mantengan vínculos con España, siempre que reúnan los demás requisitos exigibles para la obtención de un nombre de dominio.

Los nombres de dominio bajo el ".es" se asignarán al primer solicitante que tenga derecho a ello, sin que pueda otorgarse, con carácter general, un derecho preferente para la obtención o utilización de un nombre de dominio a los titulares de determinados derechos.

La asignación de un nombre de dominio confiere a su titular el derecho a su utilización, el cual estará condicionado al cumplimiento de los requisitos que en cada caso se establezcan, así como a su mantenimiento en el tiempo. La verificación por parte de la autoridad de asignación del incumplimiento de estos requisitos dará lugar a la cancelación del nombre de dominio, previa la tramitación del procedimiento que en cada caso se determine y que deberá garantizar la audiencia de los interesados.

Los beneficiarios de un nombre de dominio bajo el ".es" deberán respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del sistema de nombres de dominio bajo el ".es".

La responsabilidad del uso correcto de un nombre de dominio de acuerdo con las leyes, así como del respeto a los derechos de propiedad intelectual o industrial, corresponde a la persona u organización para la que se haya registrado dicho nombre de dominio, en los términos previstos en esta Ley. La autoridad de asignación procederá a la cancelación de aquellos nombres de dominio cuyos titulares infrinjan esos derechos o condiciones, siempre que así se ordene en la correspondiente resolución judicial, sin perjuicio de lo que se prevea en aplicación del apartado ocho de esta disposición adicional.

Cinco. En el Plan Nacional de Nombres de Dominio de Internet se establecerán mecanismos apropiados para prevenir el registro abusivo o especulativo de nombres de dominio, el aprovechamiento indebido de términos de significado genérico o topónimos y, en general, para prevenir los conflictos que se puedan derivar de la asignación de nombres de dominio.

Asimismo, el Plan incluirá las cautelas necesarias para minimizar el riesgo de error o confusión de los usuarios en cuanto a la titularidad de nombres de dominio.

A estos efectos, la entidad pública empresarial Red.es establecerá la necesaria coordinación con los registros públicos españoles. Sus titulares deberán facilitar el acceso y consulta a dichos registros públicos, que, en todo caso, tendrá carácter gratuito para la entidad.

Cinco bis. La autoridad de asignación suspenderá cautelarmente o cancelará, de acuerdo con el correspondiente requerimiento judicial previo, los nombres de dominio mediante los cuales se esté cometiendo un delito o falta tipificado en el Código Penal. Del mismo modo procederá la autoridad de asignación cuando por las Fuerzas y Cuerpos de Seguridad del Estado se le dirija requerimiento de suspensión cautelar dictado como diligencia de prevención dentro de las 24 horas siguientes al conocimiento de los hechos.

Asimismo, de acuerdo con lo dispuesto en los artículos 8, 11 y concordantes de esta Ley, la autoridad administrativa o judicial competente como medida para obtener la interrupción de la prestación de un servicio de la sociedad de la información o la retirada de un contenido, podrá requerir a la autoridad de asignación para que suspenda cautelarmente o cancele un nombre de dominio.

De la misma forma se procederá en los demás supuestos previstos legalmente.

En los supuestos previstos en los dos párrafos anteriores, sólo podrá ordenarse la suspensión cautelar o la cancelación de un nombre de dominio cuando el prestador de

servicios o persona responsable no hubiera atendido el requerimiento dictado para el cese de la actividad ilícita.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá requerir la suspensión cautelar o la cancelación. En particular, cuando dichas medidas afecten a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrán ser decididas por los órganos jurisdiccionales competentes.

La suspensión consistirá en la imposibilidad de utilizar el nombre de dominio a los efectos del direccionamiento en Internet y la prohibición de modificar la titularidad y los datos registrales del mismo, si bien podrá añadir nuevos datos de contacto. El titular del nombre de dominio únicamente podrá renovar el mismo o modificar la modalidad de renovación. La suspensión cautelar se mantendrá hasta que sea levantada o bien, confirmada en una resolución definitiva que ordene la cancelación del nombre de dominio.

La cancelación tendrá los mismos efectos que la suspensión hasta la expiración del período de registro y si el tiempo restante es inferior a un año, por un año adicional, transcurrido el cual el nombre de dominio podrá volver a asignarse.

Seis. La asignación de nombres de dominio se llevará a cabo por medios telemáticos que garanticen la agilidad y fiabilidad de los procedimientos de registro.

La presentación de solicitudes y la práctica de notificaciones se realizarán por vía electrónica, salvo en los supuestos en que así esté previsto en los procedimientos de asignación y demás operaciones asociadas al registro de nombres de dominio.

Los agentes registradores, como intermediarios en los procedimientos relacionados con el registro de nombres de dominio, podrán prestar servicios auxiliares para la asignación y renovación de éstos, de acuerdo con los requisitos y condiciones que determine la autoridad de asignación, los cuales garantizarán, en todo caso, el respeto al principio de libre competencia entre dichos agentes.

Siete. El Plan Nacional de Nombres de Dominio de Internet se aprobará mediante Orden del Ministro de Ciencia y Tecnología, a propuesta de la entidad pública empresarial Red.es.

El Plan se completará con los procedimientos para la asignación y demás operaciones asociadas al registro de nombres de dominio y direcciones de Internet que establezca el Presidente de la entidad pública empresarial Red.es, de acuerdo con lo previsto en la disposición adicional decimoctava de la Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social.

Ocho. En los términos que permitan las disposiciones aplicables, la autoridad de asignación podrá establecer un sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio, incluidos los relacionados con los derechos de propiedad industrial. Este sistema, que asegurará a las partes afectadas las garantías procesales adecuadas, se aplicará sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar.

Nueve. Con la finalidad de impulsar el desarrollo de la Administración electrónica, la entidad pública empresarial Red.es podrá prestar el servicio de notificaciones administrativas telemáticas y acreditar de forma fehaciente la fecha y hora de su recepción.

Disposición adicional séptima. *Fomento de la Sociedad de la Información.*

El Ministerio de Ciencia y Tecnología como Departamento de la Administración General del Estado responsable de la propuesta al Gobierno y de la ejecución de las políticas tendentes a promover el desarrollo en España de la Sociedad de la Información, la generación de valor añadido nacional y la consolidación de una industria nacional sólida y eficiente de productos, servicios y contenidos de la Sociedad de la Información, presentará al Gobierno para su aprobación y a las Cortes Generales un plan cuatrienal para el desarrollo de la Sociedad de la Información y de convergencia con Europa con objetivos mensurables, estructurado en torno a acciones concretas, con mecanismos de seguimiento efectivos, que aborde de forma equilibrada todos los frentes de actuación, contemplando diversos

horizontes de maduración de las iniciativas y asegurando la cooperación y la coordinación del conjunto de las Administraciones públicas.

Este plan establecerá, asimismo, los objetivos, las acciones, los recursos y la periodificación del proceso de convergencia con los países de nuestro entorno comunitario en línea con las decisiones y recomendaciones de la Unión Europea.

En este sentido, el plan deberá:

Potenciar decididamente las iniciativas de formación y educación en las tecnologías de la información para extender su uso; especialmente, en el ámbito de la educación, la cultura, la gestión de las empresas, el comercio electrónico y la sanidad.

Profundizar en la implantación del gobierno y la administración electrónica incrementando el nivel de participación ciudadana y mejorando el grado de eficiencia de las Administraciones públicas.

Disposición adicional octava. *Colaboración de los registros de nombres de dominio establecidos en España en la lucha contra actividades ilícitas.*

1. Los registros de nombres de dominio establecidos en España estarán sujetos a lo establecido en el apartado Cinco bis de la disposición adicional sexta, respecto de los nombres de dominio que asignen.

2. Las entidades de registro de nombres de dominio establecidas en España estarán obligadas a facilitar los datos relativos a los titulares de los nombres de dominio que soliciten las autoridades públicas para el ejercicio de sus competencias de inspección, control y sanción cuando las infracciones administrativas que se persigan tengan relación directa con la actividad de una página de Internet identificada con los nombres de dominio que asignen.

Tales datos se facilitarán así mismo, cuando sean necesarios para la investigación y mitigación de incidentes de ciberseguridad en los que estén involucrados equipos relacionados con un nombre de dominio de los encomendados a su gestión. Dicha información será proporcionada al órgano, organismo o entidad que se determine legal o reglamentariamente.

En ambos supuestos, la solicitud deberá formularse mediante escrito motivado en el que se especificarán los datos requeridos y la necesidad y proporcionalidad de los datos solicitados para el fin que se persigue. Si los datos demandados son datos personales, su cesión no precisará el consentimiento de su titular.

Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.

Disposición transitoria única. *Anotación en los correspondientes registros públicos de los nombres de dominio otorgados antes de la entrada en vigor de esta Ley.*

Los prestadores de servicios que, a la entrada en vigor de esta Ley, ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet deberán solicitar la anotación de, al menos, uno de ellos en el registro público en que figuraran inscritos a efectos constitutivos o de publicidad, en el plazo de un año desde la referida entrada en vigor.

Disposición final primera. *Modificación del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el párrafo a) del apartado 1 del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactada en los siguientes términos:

»a) Que los ciudadanos puedan recibir conexión a la red telefónica pública fija y acceder a la prestación del servicio telefónico fijo disponible para el público. La conexión debe ofrecer al usuario la posibilidad de emitir y recibir llamadas nacionales

e internacionales y permitir la transmisión de voz, fax y datos a velocidad suficiente para acceder de forma funcional a Internet.

A estos efectos, se considerará que la velocidad suficiente a la que se refiere el párrafo anterior es la que se utiliza de manera generalizada para acceder a Internet por los abonados al servicio telefónico fijo disponible para el público con conexión a la red mediante pares de cobre y módem para banda vocal.»

Disposición final segunda. *Modificación de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el apartado 10 de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que quedará redactado como sigue:

«10. Tasa por asignación del recurso limitado de nombres de dominio y direcciones de Internet.

a) Hecho imponible.

El hecho imponible de la tasa por asignación de nombres de dominio y direcciones de Internet estará constituido por la realización por la entidad pública empresarial Red.es de las actividades necesarias para la asignación y renovación de nombres de dominio y direcciones de Internet bajo el código de país correspondiente a España (.es).

b) Sujetos pasivos.

Serán sujetos pasivos de la tasa los solicitantes de la asignación o renovación de los nombres y direcciones de Internet.

c) Cuantía.

La cuantía de la tasa será única por cada nombre o dirección cuya asignación o renovación se solicite. En ningún caso se procederá a la asignación o a la renovación del nombre o dirección sin que se haya efectuado previamente el pago de la tasa.

Sólo podrán modificarse mediante Ley el número e identidad de los elementos y criterios de cuantificación con base en los cuales se determinan las cuotas exigibles.

A los efectos previstos en el párrafo anterior, se consideran elementos y criterios de cuantificación del importe exigible por asignación anual inicial de los nombres de dominio o direcciones de Internet el número asignado, el coste de las actividades de comprobación y verificación de las solicitudes de asignación, así como el nivel en que se produzca la asignación y, en el caso de renovación anual en los años sucesivos, el coste del mantenimiento de la asignación y de las actividades de comprobación y de actualización de datos.

Igualmente, se atenderá al número de nombres o direcciones de Internet asignados y a la actuación a través de agentes registradores para concretar la cuantía de la tasa.

El establecimiento y modificación de las cuantías resultantes de la aplicación de los elementos y criterios de cuantificación a que se refieren los párrafos anteriores podrá efectuarse mediante Orden ministerial.

No obstante lo dispuesto en los párrafos anteriores de este apartado, en los supuestos de carácter excepcional en que así esté previsto en el Plan Nacional de Nombres de Dominio de Internet y en los términos que en el mismo se fijen, con base en el especial valor de mercado del uso de determinados nombres y direcciones, la cuantía por asignación anual inicial podrá sustituirse por la que resulte de un procedimiento de licitación en el que se fijará un valor inicial de referencia estimado. Si el valor de adjudicación de la licitación resultase superior a dicho valor de referencia, aquél constituirá el importe de la tasa. En los supuestos en que se siga este procedimiento de licitación, el Ministerio de Ciencia y Tecnología requerirá, con carácter previo a su convocatoria, a la autoridad competente para el Registro de Nombres de Dominio para que suspenda el otorgamiento de los nombres y direcciones que considere afectados por su especial valor económico. A continuación, se procederá a aprobar el correspondiente pliego de bases que establecerá, tomando en consideración lo previsto en el Plan Nacional de Nombres de Dominio de Internet, los requisitos, condiciones y régimen aplicable a la licitación.

d) Devengo.

La tasa se devengará en la fecha en que se proceda, en los términos que se establezcan reglamentariamente, a la admisión de la solicitud de asignación o de renovación de los nombres o direcciones de Internet, que no se tramitará sin que se haya efectuado el pago correspondiente.

e) Exacción y gestión recaudatoria.

La exacción de la tasa se producirá a partir de la atribución de su gestión a la entidad pública empresarial Red.es y de la determinación del procedimiento para su liquidación y pago, mediante Orden ministerial.

Los modelos de declaración, plazos y formas de pago de la tasa se aprobarán mediante resolución de la entidad pública empresarial Red.es.

El importe de los ingresos obtenidos por esta tasa se destinará a financiar los gastos de la entidad pública empresarial Red.es por las actividades realizadas en el cumplimiento de las funciones asignadas a la misma en los párrafos a), b), c) y d) del apartado 4 de esta disposición, ingresándose, en su caso, el excedente en el Tesoro Público, de acuerdo con la proporción y cuantía que se determine mediante resolución conjunta de las Secretarías de Estado de Presupuestos y Gastos y de Telecomunicaciones y para la Sociedad de la Información, a propuesta de esta última.»

Disposición final tercera. *Adición de una nueva disposición transitoria a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se añade a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, una nueva disposición transitoria duodécima, con la siguiente redacción:

«Disposición transitoria duodécima. *Criterios para el desarrollo del plan de actualización tecnológica de la red de acceso de la red telefónica pública fija.*

En el plazo máximo de cinco meses a partir de la entrada en vigor de esta disposición, el operador designado para la prestación del servicio universal presentará al Ministerio de Ciencia y Tecnología, para su aprobación en el plazo de un mes, previo informe de la Comisión del Mercado de las Telecomunicaciones, un plan de actuación detallado para garantizar que las conexiones a la red telefónica pública fija posibiliten a sus abonados el acceso funcional a Internet y, en particular, a los conectados mediante Telefonía Rural de Acceso Celular (TRAC).

El desarrollo del plan estará sujeto a las siguientes condiciones:

a) Incluirá soluciones tecnológicas eficientes disponibles en el mercado para garantizar el derecho de los usuarios a disponer, previa solicitud a partir de la aprobación del plan, de la posibilidad de acceso funcional a Internet en el plazo máximo de sesenta días desde la fecha de dicha solicitud en las zonas con cobertura. Estas soluciones tecnológicas deberán prever su evolución a medio plazo hacia velocidades de banda ancha sin que ello conlleve necesariamente su sustitución.

b) La implantación en la red de acceso de las soluciones tecnológicas a las que se refiere el párrafo a) deberá alcanzar a los abonados al servicio telefónico fijo disponible al público que, en la fecha de aprobación del plan, no tienen la posibilidad de acceso funcional a Internet, de acuerdo con el siguiente calendario:

1.º Al menos al 30 por 100 antes del 30 de junio de 2003.
2.º Al menos al 70 por 100 antes del 31 de diciembre de 2003.
3.º El 100 por 100 antes del 31 de diciembre de 2004.

En todo caso, esta implantación alcanzará, al menos, al 50 por 100 de los citados abonados en cada una de las Comunidades Autónomas antes del 31 de diciembre de 2003.

c) En el plan de actuación deberá priorizarse el despliegue al que se refiere el párrafo b) con arreglo al criterio de mayor densidad de abonados afectados.

d) A los efectos de lo dispuesto en los apartados anteriores y en caso de que sea necesario, el operador designado para la prestación del servicio universal podrá concluir con otros operadores titulares de concesiones de dominio público radioeléctrico, contratos de cesión de derechos de uso de las bandas de frecuencias necesarias para el cumplimiento de los objetivos establecidos en esta disposición. Dichos contratos deberán ser sometidos a la previa aprobación por parte del Ministerio de Ciencia y Tecnología, que podrá establecer las condiciones de salvaguarda del interés público que estime necesarias.»

Disposición final cuarta. *Modificación de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el último párrafo de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactado de la siguiente forma:

«Igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango a la presente Ley se opongan a lo dispuesto en ella y, en especial, a lo dispuesto en el artículo 37.1.ª), en lo relativo a la velocidad de transmisión de datos.»

Disposición final quinta. *Adecuación de la regulación reglamentaria sobre contratación telefónica o electrónica con condiciones generales a esta Ley.*

El Gobierno, en el plazo de un año, modificará el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, para adaptar su contenido a lo dispuesto en esta Ley.

En dicha modificación, el Gobierno tendrá especialmente en cuenta la necesidad de facilitar la utilización real de los contratos electrónicos, conforme al mandato recogido en el artículo 9.1 de la Directiva 2000/31/CE.

Disposición final sexta. *Fundamento constitucional.*

Esta Ley se dicta al amparo del artículo 149.1.6.ª, 8.ª y 21.ª de la Constitución, sin perjuicio de las competencias de las Comunidades Autónomas.

Disposición final séptima. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar mediante Reglamento lo previsto en esta Ley.

Disposición final octava. *Distintivo de adhesión a códigos de conducta que incorporen determinadas garantías.*

En el plazo de un año a partir de la entrada en vigor de esta Ley, el Gobierno aprobará un distintivo que permita identificar a los prestadores de servicios que respeten códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyan, entre otros contenidos, la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respeten los principios establecidos en la normativa comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores, en los términos que reglamentariamente se establezcan.

Disposición final novena. *Entrada en vigor.*

Esta Ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

No obstante, las disposiciones adicional sexta y finales primera, segunda, tercera y cuarta de esta Ley entrarán en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

ANEXO

Definiciones

A los efectos de esta Ley, se entenderá por:

a) "Servicios de la sociedad de la información" o "servicios": todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.

2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3.º La gestión de compras en la red por grupos de personas.

4.º El envío de comunicaciones comerciales.

5.º El suministro de información por vía telemática.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.

2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.ª) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.º Los servicios de radiodifusión sonora, y

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

b) "Servicio de intermediación": servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

c) "Prestador de servicios" o "prestador": persona física o jurídica que proporciona un servicio de la sociedad de la información.

d) "Destinatario del servicio" o "destinatario": persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

e) "Consumidor": persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

f) "Comunicación comercial": toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

g) "Profesión regulada": toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

h) "Contrato celebrado por vía electrónica" o "contrato electrónico": todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

i) "Ámbito normativo coordinado": todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1.º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado, y

2.º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidos en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

j) "Órgano competente": todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas.

§ 13

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información

Jefatura del Estado
«BOE» núm. 312, de 29 de diciembre de 2007
Última modificación: 12 de noviembre de 2020
Referencia: BOE-A-2007-22440

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

PREÁMBULO

I

La presente Ley se enmarca en el conjunto de medidas que constituyen el Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, Plan Avanza, aprobado por el Gobierno en noviembre de 2005.

El Plan Avanza prevé entre sus medidas la adopción de una serie de iniciativas normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y de las comunicaciones y para garantizar los derechos de los ciudadanos en la nueva sociedad de la información.

En esta línea, la presente Ley, por una parte, introduce una serie de innovaciones normativas en materia de facturación electrónica y de refuerzo de los derechos de los usuarios y, por otra parte, acomete las modificaciones necesarias en el ordenamiento jurídico para promover el impulso de la sociedad de la información.

En este sentido, se introducen una serie de modificaciones tanto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, como de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que constituyen dos piezas angulares del marco jurídico en el que se desenvuelve el desarrollo de la sociedad de la información.

Dicha revisión del ordenamiento jurídico se completa con otras modificaciones menores de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones y de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista.

II

El capítulo I de la Ley introduce sendos preceptos dirigidos a impulsar el empleo de la factura electrónica y del uso de medios electrónicos en todas las fases de los procesos de contratación y a garantizar una interlocución electrónica de los usuarios y consumidores con las empresas que presten determinados servicios de especial relevancia económica.

En materia de facturación electrónica, el artículo 1 establece la obligatoriedad del uso de la factura electrónica en el marco de la contratación con el sector público estatal en los términos que se precisen en la Ley reguladora de contratos del sector público, define el concepto legal de factura electrónica y, asimismo, prevé actuaciones de complemento y profundización del uso de medios electrónicos en los procesos de contratación.

Así, el citado precepto prevé que el Gobierno determinará el órgano competente de la Administración General del Estado que impulsará el empleo de la factura electrónica entre los diversos agentes del mercado, en particular entre las pequeñas y medianas empresas y en las denominadas microempresas, de acuerdo con la definición establecida en la Recomendación C(2003) 1422 de la Comisión Europea, de 6 de mayo de 2003, con el fin de fomentar el desarrollo del comercio electrónico. Por su parte, las Comunidades Autónomas, de acuerdo con las competencias que tenga reconocidas por sus Estatutos, colaborarán en coordinación con la Administración del Estado en el empleo de la factura electrónica.

De igual modo el Gobierno, o en su caso las Comunidades Autónomas en el ámbito de sus competencias desarrollarán, en cooperación con las asociaciones representativas de las empresas proveedoras de soluciones técnicas de facturación electrónica y de las asociaciones relevantes de usuarios, un plan para la generalización del uso de la factura electrónica en España, definiendo, asimismo, los contenidos básicos de dicho plan.

Asimismo, la Ley habilita a los Ministerios de Industria, Turismo y Comercio y de Economía y Hacienda, respetando las competencias reconocidas a las Comunidades Autónomas, para que aprueben las normas sobre formatos estructurados estándar de facturas electrónicas que sean necesarias para facilitar la interoperabilidad tanto en el sector público como en el sector privado y permitan facilitar y potenciar el tratamiento automatizado de las mismas.

Además, el citado precepto, yendo más allá del impulso a la extensión del uso de la factura electrónica, encomienda a las diversas Administraciones Públicas en el ámbito de sus competencias la promoción de la extensión y generalización del uso de medios electrónicos en las demás fases de los procesos de contratación.

El artículo 2, por su parte, establece la obligación de las empresas de determinados sectores con especial incidencia en la actividad económica (entre otras, compañías dedicadas al suministro de electricidad, agua y gas, telecomunicaciones, entidades financieras, aseguradoras, grandes superficies, transportes, agencias de viaje) de facilitar un medio de interlocución telemática a los usuarios de sus servicios que cuenten con certificados reconocidos de firma electrónica.

Esta nueva obligación tiene por finalidad asegurar que los ciudadanos cuenten con un canal de comunicación electrónica con las empresas cuyos servicios tienen una mayor trascendencia en el desarrollo cotidiano de sus vidas.

A tales efectos, se especifica que dicha interlocución telemática ha de facilitar al menos la realización de trámites tales como la contratación electrónica, modificación de condiciones contractuales, altas, bajas, quejas, histórico de facturación, sustitución de informaciones y datos en general, así como el ejercicio de sus derechos de acceso, rectificación, oposición y cancelación en materia de protección de datos. Asimismo, se prevé que dicho medio de interlocución telemática sirva para sustituir los trámites que actualmente se realicen por fax. No obstante, el citado precepto no impide que excepcionalmente las empresas obligadas por el mismo no faciliten la contratación de productos o servicios que por su naturaleza no sean susceptibles de comercialización por vía electrónica.

Esta obligación vendrá a complementar la garantía del derecho de una comunicación electrónica de los ciudadanos con las Administraciones Públicas, establecida en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en ejecución de uno de los mandatos normativos contenidos en el Plan Avanza.

Por último, el artículo 3 tiene por finalidad establecer una regulación mínima de las subastas electrónicas entre empresarios (B2B) a fin de establecer un marco jurídico que dote a esta técnica de compra de la necesaria transparencia y seguridad jurídica.

En este sentido, la regulación prevista tiene por objeto evitar las suspicacias de las empresas a la hora de participar en estos nuevos métodos de compra y eliminar cualquier tipo de práctica o competencia desleal. En definitiva, se trata de garantizar a través de un precepto específico los principios de igualdad de trato, de no discriminación y transparencia entre empresas.

III

El capítulo II de la Ley engloba las modificaciones legislativas que se han estimado necesarias para promover el impulso de la sociedad de la información y de las comunicaciones electrónicas.

Dichas modificaciones afectan principalmente a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y a la Ley 59/2003, de 19 de diciembre, de firma electrónica, si bien se incluyen también modificaciones de menor entidad de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista para incluir un nuevo tipo de infracción que respalde lo dispuesto en el artículo 2 de la presente Ley, se introducen una serie de cambios en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones y se introducen, asimismo, modificaciones en la Ley de Propiedad Intelectual.

El artículo 4 de la Ley incluye las diferentes modificaciones necesarias en el vigente texto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

Estas modificaciones tienen como finalidad, en primer lugar, revisar o eliminar obligaciones excesivas o innecesarias y, en segundo lugar, flexibilizar las obligaciones referidas a las comunicaciones comerciales y a la contratación electrónicas a fin de, entre otras razones, adecuar su aplicación al uso de dispositivos móviles.

La primera medida prevista es la nueva redacción del artículo 8 que regula las restricciones a la prestación de servicios de la sociedad de la información y su procedimiento de cooperación intracomunitario. Por lo que al primer aspecto se refiere, es decir, las restricciones a los servicios de telecomunicaciones, este precepto establece que en el caso de que un determinado servicio de esta naturaleza atente contra los principios que en el propio precepto se recogen, los órganos competentes para su protección adoptarán las medidas necesarias para que se pueda interrumpir su prestación o retirar los datos que los vulneran. Los principios objeto de protección son: la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional; la protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores y usuarios; el respeto a la dignidad de la persona y al principio a la no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y finalmente, la protección de la juventud y de la infancia. Como no puede ser de otra manera, se prevé que en la adopción de estas medidas se respetarán siempre las garantías y procedimientos establecidos en las leyes. Finalmente, sobre este punto de las restricciones a la prestación de servicios de la Sociedad de la Información, el artículo 8 incorpora además el principio de que solo la autoridad judicial competente, en los casos en que la Constitución y las leyes de los respectivos derechos y libertades fundamentales así lo prevean de forma excluyente, podrán adoptar las medidas restrictivas previstas en este artículo, en tanto que garante de los derechos a la libertad de expresión, de producción y creación literaria científica y técnica, de información y de cátedra.

En relación con el procedimiento de cooperación intracomunitario, el vigente apartado 4 del artículo 8 mantiene prácticamente su redacción pues constituye una transposición necesaria del procedimiento intracomunitario de cooperación previsto en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Por su parte, el vigente apartado 2 del artículo 8, sobre colaboración de prestadores de servicios de intermediación para impedir

el acceso desde España a servicios o contenidos cuya interrupción o retirada haya decidido un órgano competente, se traslada al artículo 11.

En coherencia con la nueva redacción del artículo 8 se elimina también el párrafo a) del apartado 2 del artículo 38, por el que se tipifica como infracción administrativa muy grave el incumplimiento de las órdenes dictadas por órganos administrativos en virtud del artículo 8. A este respecto, se considera que los órganos competentes para imponer restricciones en el mundo físico, ya sean judiciales o administrativos -piénsese por ejemplo en las autoridades de control sanitario-, deberán estar habilitados por sus propias normas a imponer dichas restricciones a los prestadores de servicios de la sociedad de la información cuando incumplan una orden emanada por los mismos en ejercicio de sus competencias legalmente atribuidas. Sin perjuicio de lo anterior, la nueva redacción del apartado 4 del artículo 8 remite al artículo 11 para habilitar al órgano competente a requerir la colaboración de los prestadores de servicios de intermediación en caso de estimarlo necesario para garantizar la eficacia de las medidas que hubiera adoptado.

Como consecuencia de las modificaciones realizadas en el artículo 8 se procede a hacer un ajuste técnico en la remisión contenida en el artículo 4 que ahora debe remitirse al artículo 11.

La segunda modificación importante prevista en relación con la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) es la supresión de la obligación establecida en el artículo 9 sobre constancia registral de los nombres de dominio, dado que se ha revelado como poco operativa desde un punto de vista práctico.

En coherencia con la supresión del artículo 9 se prevé también la eliminación del párrafo a) del apartado 4 del artículo 38 en el que se tipifica como infracción administrativa leve el incumplimiento de lo dispuesto en el artículo 9.

Como consecuencia de la supresión del artículo 9 se procede a una modificación técnica en la redacción del párrafo b) del apartado 1 del artículo 10. Asimismo, se realiza un ajuste de redacción en el párrafo f) del apartado 1 del artículo 10.

En tercer lugar, se ha entendido necesaria la modificación del artículo 11. La redacción vigente del artículo incluye una posibilidad de intervención del Ministerio de Ciencia y Tecnología (hoy Ministerio de Industria, Turismo y Comercio) que se ha eliminado. En este sentido, son los propios órganos competentes los que en ejercicio de las competencias que legalmente tengan atribuidas deben dirigirse directamente a los prestadores de servicios de intermediación, sin que sea necesario que un departamento ajeno, como es el Ministerio de Industria, Turismo y Comercio, intervenga en un procedimiento en el que se diluciden asuntos en los que carece de competencias.

Por otra parte, se precisa en el artículo 11 que la suspensión del servicio que se puede ordenar a los prestadores de servicios de intermediación se circunscribe a aquéllos empleados por terceros para proveer el servicio de la sociedad de la información o facilitar el contenido cuya interrupción o retirada haya sido ordenada. Se añade, además, un nuevo apartado 2, que traslada a este artículo la previsión actualmente establecida en el apartado 2 del artículo 8, que prevé la posibilidad de requerir la colaboración de los prestadores de servicios de intermediación para impedir el acceso desde España a servicios o contenidos cuya interrupción o retirada haya sido decidida.

Igualmente se incluye un nuevo inciso en el apartado 3 del artículo 11 que aclara que la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

Por otra parte, se incluye un nuevo artículo 12 bis que establece la obligación de los proveedores de acceso a Internet establecidos en España a informar a sus usuarios sobre los medios técnicos que permitan, entre otros, la protección frente a virus informáticos y programas espía, la restricción de los correos electrónicos no solicitados, y la restricción o selección del acceso a determinados contenidos y servicios no deseados o nocivos para la juventud y la infancia.

Igualmente, se obliga a dichos prestadores, así como a los prestadores de servicios de correo electrónico a informar a sus clientes sobre las medidas de seguridad que aplican en la provisión de sus servicios.

Asimismo, se encomienda a los proveedores de servicios de acceso la función de informar a sus clientes sobre las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial. A fin de respaldar estas obligaciones se incluye un nuevo tipo de infracción leve en el apartado 4 del artículo 38, que, teniendo en cuenta la supresión del vigente párrafo a), dará nuevo contenido al mismo.

Otra modificación considerada necesaria es la revisión de la vigente redacción del apartado 2 del artículo 17 a fin de aclarar y precisar que en virtud del mismo se responsabiliza al proveedor del link o del motor de búsqueda de los contenidos de los que tiene conocimiento cuando hayan sido elaborados bajo su «dirección, autoridad o control».

Se incorpora una nueva redacción al apartado 3 del artículo 18, en el sentido de que los códigos de conducta a que se refiere este precepto deberán ser accesibles por vía electrónica, fomentándose su traducción en las distintas lenguas oficiales del Estado y de la Unión Europea con el fin de proporcionarles la mayor difusión posible.

En materia de comunicaciones comerciales se flexibiliza la exigencia de información prevista en el vigente artículo 20 sobre mensajes publicitarios a través de correo electrónico o medios de comunicación equivalentes de modo que en vez de la inserción del término «publicidad» al inicio del mensaje pueda incluirse la abreviatura «publi». Se trata de una medida que ha sido solicitada en diversas ocasiones por agentes que desarrollan actividades relacionadas con la publicidad a través de telefonía móvil y, por otra parte, no supone menoscabo de la protección y de los derechos de información de los usuarios, ya que el término «publi» es fácilmente reconocible como indicativo de «publicidad».

Adicionalmente, se realizan ajustes menores en la redacción del mencionado artículo a fin de alinearlo en mayor medida con lo dispuesto en la Directiva 2000/31/CE.

En materia de contratación electrónica se realiza un ajuste de la redacción actual del artículo 24 a fin de incluir una remisión expresa a la Ley 59/2003, de 19 de diciembre, de firma electrónica y destacar así el especial valor probatorio de los contratos electrónicos que sean celebrados mediante el uso de instrumentos de firma electrónica.

De igual modo, se ajusta el artículo 27, relativo a las obligaciones de información previa en materia de contratación electrónica, a la luz de la experiencia acumulada en su aplicación por parte del Ministerio de Industria, Turismo y Comercio en ejercicio de sus competencias de inspección y control de páginas de Internet. En este sentido, se prevé que la información que debe facilitarse ha de «ponerse a disposición» de los usuarios «mediante técnicas adecuadas al medio de comunicación utilizado», flexibilizando de este modo la redacción anterior con vistas a facilitar la realización de operaciones de contratación electrónica mediante dispositivos que cuenten con pantallas de visualización de formato reducido.

Asimismo, se incluye en la nueva redacción del artículo 27 una regla aclaratoria por la cual, cuando el prestador de servicios diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderán cumplidas las obligaciones de información previa establecidas en dicho precepto cuando el citado prestador facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

También se modifica el apartado 2 del artículo 27 a fin de eliminar el inciso «cuando no se utilicen estos medios con el exclusivo propósito de eludir el cumplimiento de dicha obligación» dado que en la práctica es imposible determinar cuando se hace con este propósito.

Este artículo 4 modifica también los artículos 33, 35 y 43 de la Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y del Comercio Electrónico.

Las modificaciones que se introducen a los artículos 33 y 35 tienen por objeto adaptar su contenido a la vigente organización de la Administración territorial del Estado en función de las competencias que tienen atribuidas tanto la Administración General del Estado como aquellas de las Comunidades Autónomas.

Por otra parte, se da una nueva redacción al artículo 43 de la Ley 34/2002 que se refiere a la potestad sancionadora. En concreto, la nueva redacción establece que la imposición de sanciones por incumplimiento de lo establecido en dicha ley corresponderá al órgano o autoridad que dictó la resolución incumplida o al que estén adscritos los inspectores. En el ámbito de las Comunidades Autónomas, las infracciones contra derechos y garantías de los consumidores y usuarios serán sancionadas por los órganos correspondientes en materia de consumo.

Además, se incorpora una nueva redacción a la disposición adicional tercera de la mencionada Ley sobre el sistema arbitral de consumo en el sentido de que los prestadores y destinatarios de los servicios de la sociedad de la información pueden someter sus conflictos a este sistema de resolución.

Finalmente se revisa, actualiza y amplía el contenido de la actual disposición adicional quinta referida a la accesibilidad de las páginas de Internet, a fin de garantizar adecuadamente la accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos.

IV

El artículo 5 de la Ley contempla las modificaciones necesarias en el articulado de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estas modificaciones tienen por objeto clarificar las reglas de valoración de la firma electrónica en juicio y flexibilizar la obligación de los prestadores de servicios de certificación de comprobar los datos inscritos en registros públicos a fin de eliminar cargas excesivas.

El primer aspecto que se revisa del artículo 3 de la Ley de firma electrónica es la definición de «documento electrónico» que se modifica para alinearla en mayor medida con los conceptos utilizados en otras normas españolas de carácter general y en los países de nuestro entorno.

En segundo lugar, se aclara la redacción del apartado 8 del artículo 3, especificando que lo que debe comprobarse, en caso de impugnarse en juicio una firma electrónica reconocida, es si concurren los elementos constitutivos de dicho tipo de firma electrónica, es decir, que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados electrónicos, y que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La tercera modificación acometida es la revisión de la regla de exención de responsabilidad establecida en el segundo inciso del apartado 5 del artículo 23 de la Ley que resulta en exceso rígida y onerosa para los prestadores de servicios de certificación, por lo que se procede a su oportuna flexibilización.

En coherencia con la mencionada modificación del artículo 23, se corrige asimismo el artículo 13, previendo que para la comprobación de los datos relativos a las personas jurídicas y a la representación de las mismas será suficiente que sean aportados y cotejados los documentos públicos en los que figuren los citados datos, estableciendo así un nivel de exigencia equiparable al empleado por las propias Administraciones Públicas en el cotejo y bastanteo de ese tipo de datos.

Se introduce, además, una modificación técnica de la actual redacción del apartado 4 del artículo 31.

Por último, al igual que en el caso de la Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y del Comercio Electrónico, este artículo incorpora una disposición adicional undécima a la Ley de Firma Electrónica sobre resolución de conflictos en el sentido de que los usuarios y prestadores de servicios de certificación podrán someter las desavenencias que se susciten entre los mismos al procedimiento arbitral.

V

El artículo 6 incluye un nuevo tipo de infracción en el artículo 64 de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, a fin de respaldar la nueva obligación de disponer de un medio de interlocución electrónica para la prestación de servicios al público de especial trascendencia económica establecido en el artículo 2 de la presente Ley.

El artículo 7 de la Ley, introduce una serie de modificaciones en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

La primera de estas modificaciones afecta al apartado primero del artículo 22 letras a) y c) cuya finalidad es asegurar el acceso a los servicios telefónicos y de Internet como servicio universal. Mediante la redacción de la letra a) del artículo 22 apartado 1 se garantiza que todos usuarios finales puedan obtener una conexión a la red pública desde una ubicación fija y acceder a la prestación de servicio telefónico. La conexión debe ofrecer al usuario la posibilidad de efectuar y recibir llamadas telefónicas y permitir comunicaciones de fax y datos de velocidad suficiente para acceder a Internet, debiendo permitir dicha conexión comunicaciones en banda ancha en los términos definidos por la normativa vigente.

La redacción de la letra c) del citado precepto, garantiza tanto la existencia de una oferta suficiente de teléfonos públicos de pago en todo el territorio nacional, que satisfaga la necesidades de los usuarios, en cobertura geográfica y en número de aparatos, la accesibilidad de dichos teléfonos por los usuarios con discapacidades, como la calidad de los servicios con la posibilidad de efectuar gratuitamente llamadas de emergencia y finalmente la existencia de una oferta suficiente de equipos terminales de acceso a Internet de banda ancha en los términos que establezca la legislación en vigor.

Con el fin de reforzar los derechos de los usuarios frente a los proveedores de redes y servicios de comunicaciones electrónicas, se modifican los artículos 53 y 54 de la Ley General de Telecomunicaciones, mediante la tipificación como infracción administrativa del incumplimiento por parte de los operadores de los derechos de los consumidores y usuarios en el ámbito de las telecomunicaciones.

Asimismo, se reestablece la exención de la antigua tasa por reserva de uso especial del espectro, a radioaficionados y usuarios de la Banda Ciudadana CB-27 que figuraba en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, para aquellos usuarios que a la fecha de devengo hubieran cumplido los 65 años de edad, así como a los beneficiarios de una pensión pública o que tengan reconocido un grado de minusvalía igual o superior al 33 por 100.

El artículo 8 establece un nuevo régimen aplicable a las tarifas por las tareas de asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España, que pasarán a tener la consideración de precio público. Con ello, se permite a la entidad pública empresarial Red.es comercializar los nombres de dominio «.es» en las mismas condiciones en las que se comercializan el resto de nombres de dominio genéricos y territoriales.

La disposición adicional primera prevé que la autoridad de asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España («.es») adopte las medidas que sean necesarias para asegurar que puedan asignarse nombres de dominio que contengan caracteres propios de las lenguas oficiales de España distintos de los incluidos en el alfabeto inglés, como es la letra «ñ» o la «ç», en un plazo máximo de 3 meses desde la entrada en vigor de esta Ley.

La disposición adicional segunda prevé que el Gobierno, en colaboración con las Comunidades Autónomas, impulsará la extensión de la banda ancha con el fin de conseguir antes del 31 de diciembre de 2008, una cobertura de servicio universal de banda ancha, para todos los ciudadanos, independientemente del tipo de tecnología utilizada en su caso y su ubicación geográfica. La acción del Gobierno deberá dirigirse prioritariamente a las áreas en las que la acción de los mecanismos del mercado sea insuficiente.

Asimismo, se especifica que el Gobierno analizará de forma continua las diferentes opciones tecnológicas y las condiciones de provisión de servicios de acceso a Internet de banda ancha. Para ello, se colaborará con los diferentes sectores interesados a fin de que asesoren al Gobierno en la elaboración de un informe anual sobre la situación del uso de los servicios de acceso a Internet de banda ancha en España que tendrá carácter público y podrá incluir recomendaciones para acelerar el despliegue de estos servicios. Estos análisis e informes deberán elaborarse de forma territorializada por Comunidades autónomas, compartiéndose los datos en formato electrónico con las Administraciones que lo soliciten.

Por su parte, la disposición adicional tercera prevé que el Gobierno elabore en el plazo de seis meses un Plan para la mejora de los niveles de seguridad y confianza en Internet,

que incluirá directrices y medidas para aumentar la seguridad frente a las amenazas de Internet y proteger la privacidad on line.

La disposición adicional cuarta se refiere a las funciones de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y a los órganos estadísticos de las Comunidades Autónomas en materia de requerimientos de información para fines estadísticos y de análisis. A estos efectos se atribuye a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información tanto la facultad de recabar de los agentes que operan en el sector de las tecnologías de la información y de la sociedad de la información en general la información necesaria para el ejercicio de sus funciones como la potestad de sancionar las infracciones consistentes en no facilitar al mismo la información requerida.

En la disposición adicional quinta se establece la obligación de que en la elaboración de los proyectos de obras de construcción de carreteras o de infraestructuras ferroviarias se prevea la instalación de canalizaciones para el despliegue de redes de comunicaciones electrónicas a lo largo de toda la longitud de las mismas y del equipamiento para asegurar la cobertura de comunicaciones móviles en todo su recorrido. Estas canalizaciones deberán ponerse a disposición de los operadores de redes y servicios de comunicaciones electrónicas interesados en condiciones equitativas, no discriminatorias, neutrales y orientadas a costes.

La disposición adicional sexta encomienda al Ministerio de Industria, Turismo y Comercio la función de mantener una base de datos actualizada y sectorializada como mínimo por ámbitos territoriales de Comunidad autónoma sobre el despliegue y cobertura de infraestructuras y servicios de comunicaciones electrónicas y de la sociedad de la información en España.

La disposición adicional séptima establece que la constitución de la Agencia Estatal de Radiocomunicaciones tendrá lugar en el momento que se señale en el Real Decreto de aprobación de su Estatuto.

La disposición adicional octava modifica el apartado 13 del artículo 48 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. La norma establece en Barcelona la sede de la Comisión del Mercado de las Telecomunicaciones que dispondrá de patrimonio independiente del patrimonio del Estado. Con la introducción de esta disposición se otorga rango de ley al establecimiento de la sede de dicha Comisión.

Las disposiciones adicionales novena y décima modifican, respectivamente, la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada y el texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre al objeto de rebajar de manera drástica los tiempos de constitución de una sociedad limitada pudiéndose reducir hasta cuatro días.

En concreto, la modificación se basa en las siguientes medidas: (i) Introducción de un modelo tipo u orientativo de estatutos en la sociedad de responsabilidad limitada; (ii) agilización de los trámites que implican la obtención de una denominación social como paso previo a la constitución de una sociedad de responsabilidad limitada, sin por ello restar importancia a la seguridad que aporta al tráfico mercantil el sistema vigente de denominaciones sociales, tutelado por el Registro Mercantil Central; y (iii) facultar a los administradores, desde el otorgamiento de la escritura fundacional, para el desarrollo del objeto social y para la realización de toda clase de actos y contratos relacionados con el mismo.

Esta disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información.

La disposición adicional undécima introduce un aspecto de significativa relevancia ya que mandata a las Administraciones Públicas a promover el impulso, el desarrollo y la

aplicación de los estándares de accesibilidad para las personas con discapacidad en los diseños y procesos basados en las nuevas tecnologías de la sociedad de la información.

Para garantizar el derecho de los ciudadanos a la utilización de las distintas lenguas del Estado, la disposición adicional duodécima impone a las Administraciones Públicas el deber de fomentar el pluralismo lingüístico en la sociedad de la información y la decimotercera establece, con el fin de impulsar los medios electrónicos propios de estas tecnologías, la obligación de regular los instrumentos telemáticos necesarios para ser utilizados por aquellos profesionales colegiados que elaboren y preparen proyectos e informes que hayan de incorporarse a los procedimientos que tramiten las Administraciones Públicas.

La disposición adicional decimocuarta atribuye al Centro Nacional de Referencia de Aplicación de las Tecnologías de Información y Comunicación (CENATIC), en colaboración con los Centros Autónomos de referencia y con el Centro de Transferencia de Tecnología entre Administraciones Públicas de la Administración General del Estado la difusión de las aplicaciones declaradas de fuente abierta por las propias Administraciones Públicas. Igualmente, el CENATIC se encargará del asesoramiento sobre los aspectos jurídicos, tecnológicos y metodológicos para la liberación del software y conocimiento.

Con objeto de fomentar la participación de la sociedad y de las entidades privadas sin ánimo de lucro y garantizar el pluralismo y la libertad de expresión en la sociedad de la información, la Ley incluye una disposición adicional decimoquinta en cuya virtud se establecerán los medios de apoyo y líneas de financiación para el desarrollo de los servicios de la sociedad de la información promovidos por estas entidades y que fomenten los valores democráticos, la participación ciudadana y atiendan al interés general o presten servicios a grupos sociales desfavorecidos.

La disposición adicional decimosexta se refiere a la puesta a disposición de los ciudadanos, en los términos legalmente establecidos de los contenidos digitales de las Administraciones Públicas de cuyos derechos de propiedad intelectual sean titulares o pertenezcan al dominio público.

La disposición adicional decimoséptima ofrece la posibilidad tanto a las personas físicas como jurídicas de poner a disposición del público los contenidos de las obras digitalizadas de las que sean titulares, con la finalidad de fomentar las nuevas tecnologías y la sociedad de la información entre los ciudadanos.

CAPÍTULO I

Medidas de impulso de la sociedad de la información

Artículo 1. *Medidas de impulso de la factura electrónica y del uso de medios electrónicos en otras fases de los procesos de contratación.*

1. La facturación electrónica en el marco de la contratación con el sector público estatal será obligatoria en los términos que se establezcan en la Ley reguladora de la contratación en el sector público y en su normativa de desarrollo.

A estos efectos, se entenderá que la factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor.

2. El Gobierno determinará el órgano competente de la Administración General del Estado que impulsará el empleo de la factura electrónica entre empresarios, profesionales y demás agentes del mercado, en particular, entre las pequeñas y medianas empresas y en las denominadas microempresas, con el fin de fomentar el desarrollo del comercio electrónico. Las Comunidades Autónomas, de acuerdo con las competencias que tengan reconocidas por sus Estatutos, colaborarán en coordinación con la Administración del Estado en el impulso del empleo de la factura electrónica.

El Gobierno, o en su caso las Comunidades Autónomas en el ámbito de sus competencias, establecerán, en un plazo máximo de nueve meses desde la entrada en vigor de esta Ley -o en el plazo que en su lugar establezca la Administración competente-, en coordinación con las Comunidades Autónomas -cuando no les corresponda la elaboración

propia- y previa consulta a las asociaciones relevantes representativas de las entidades proveedoras de soluciones técnicas de facturación electrónica, a las asociaciones relevantes de usuarios de las mismas y a los colegios profesionales que agrupen a técnicos del sector de la Sociedad de la Información y de las Telecomunicaciones, un plan para la generalización del uso de la factura electrónica en España.

El citado Plan contendrá, entre otros, los criterios de accesibilidad y promoverá la interoperabilidad de las distintas soluciones de facturación electrónica. El Plan de la Administración General del Estado establecerá esquemas específicos de ayudas económicas para la implantación de la factura electrónica, en los cuales se contemplarán unos fondos generales para las Comunidades Autónomas que desarrollen su propio Plan para la generalización del uso de la factura electrónica, y serán estas últimas las que precisarán los destinos y condiciones de tramitación y concesión de las ayudas derivadas de estos fondos.

3. Los Ministerios de Industria, Turismo y Comercio y de Economía y Hacienda, teniendo en cuenta las competencias reconocidas a las Comunidades Autónomas, aprobarán, en un plazo máximo de 6 meses desde la entrada en vigor de esta Ley, las normas sobre formatos estructurados estándar de facturas electrónicas que sean necesarias para facilitar la interoperabilidad del sector público con el sector privado y favorecer y potenciar el tratamiento automatizado de las mismas. Estas normas no serán restrictivas y fomentarán que el sector público adopte los formatos de amplia implantación definidos por las organizaciones de estandarización globales pertinentes.

Los formatos estructurados de las facturas electrónicas permitirán su visualización y emisión en las distintas lenguas oficiales existentes, con la finalidad de garantizar los derechos de los usuarios.

4. Además, las diversas Administraciones Públicas promoverán en el ámbito de sus competencias y según su criterio la incorporación de la factura electrónica en las diferentes actuaciones públicas distintas de la contratación, en particular, en materia de justificación de ayudas y subvenciones.

5. Será de aplicación al tratamiento y conservación de los datos necesarios para la facturación electrónica lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo.

Artículo 2. *Obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica.*

1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio seguro de interlocución telemática que les permita la realización de, al menos, los siguientes trámites:

a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.

b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.

c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.

d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

2. A los efectos de lo dispuesto en el apartado anterior, tendrán la consideración de empresas que presten servicios al público en general de especial trascendencia económica, las que agrupen a más de cien trabajadores o su volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.010.121,04 euros y que, en ambos casos, operen en los siguientes sectores económicos:

a) Servicios de comunicaciones electrónicas a consumidores, en los términos definidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

b) Servicios financieros destinados a consumidores, que incluirán los servicios bancarios, de crédito o de pago, los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros. En particular, se entenderá por:

1. Servicios bancarios, de crédito o de pago: las actividades relacionadas en el artículo 52 de la Ley 26/1988, de 29 de julio, sobre Disciplina e Intervención de las Entidades de Crédito.
2. Servicios de inversión: los definidos como tales en la Ley 24/1988, de 28 de julio, del Mercado de Valores.
3. Operaciones de seguros privados: las definidas en el artículo 3 del texto refundido de la Ley de ordenación y supervisión de los seguros privados, aprobado por Real Decreto Legislativo 6/2004, de 29 de octubre.
4. Planes de pensiones: los definidos en el artículo 1 del texto refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre.
5. Actividad de corredor de seguros: la definida en la Ley 26/2006, de 17 de julio, de mediación en seguros y reaseguros privados.

c) Servicios de suministro de agua a consumidores, definidos de acuerdo con la normativa específica.
d) Servicios de suministro de gas al por menor, de acuerdo con lo dispuesto en la Ley 34/1998, de 7 de octubre, del Sector de Hidrocarburos.
e) Servicios de suministro eléctrico a consumidores finales, de acuerdo con lo dispuesto en el título VIII de la Ley 54/1997, de 27 noviembre, del Sector Eléctrico.
f) Servicios de agencia de viajes, de acuerdo con lo dispuesto en el Real Decreto 271/1988, de 25 de marzo, por el que se regula el ejercicio de las actividades propias de las agencias de viajes.
g) Servicios de transporte de viajeros por carretera, ferrocarril, por vía marítima, o por vía aérea, de acuerdo con lo dispuesto en la normativa específica aplicable.
h) Actividades de comercio al por menor, en los términos fijados en el apartado 2 del artículo 1 de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista y en su normativa de desarrollo, a las que serán de aplicación únicamente los apartados c) y d) del apartado 1 del presente artículo.

3. Excepcionalmente, el Gobierno o, en su caso, los órganos competentes de las Comunidades Autónomas podrán ampliar el ámbito de aplicación del apartado 1 del presente artículo a otras empresas diferentes de las previstas en la Ley, en aquellos casos en los que, por la naturaleza del servicio que presten, se considere que en el desarrollo de su actividad normal deban tener una interlocución telemática con sus clientes o usuarios.
En el plazo de un año desde la entrada en vigor de la obligación a que se refiere el apartado 1, el Gobierno analizará la aplicación del apartado 2 de este artículo a otras empresas con más de cien trabajadores o que tengan un volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, superior a 6.010.212,04 euros, que en el desarrollo de su actividad normal, presten servicios en los que se considere que deban tener una interlocución telemática con sus clientes o usuarios.
Las Comunidades Autónomas con competencias exclusivas en las materias objeto de obligación de comunicación telemática podrán modificar el ámbito y la intensidad de aplicación del apartado 1 del presente artículo en aquellos casos en que precisamente debido al desarrollo sectorial de sus competencias lo consideren oportuno.

Artículo 2 bis. *Factura electrónica en el sector privado.*

A efectos de lo dispuesto en esta Ley:

1. Las empresas prestadoras de los servicios a que alude el artículo 2.2, deberán expedir y remitir facturas electrónicas en sus relaciones con empresas y particulares que acepten recibirlas o que las hayan solicitado expresamente. Este deber es independiente del tamaño de su plantilla o de su volumen anual de operaciones.

No obstante, las agencias de viaje, los servicios de transporte y las actividades de comercio al por menor sólo están obligadas a emitir facturas electrónicas en los términos previstos en el párrafo anterior cuando la contratación se haya llevado a cabo por medios electrónicos.

Las obligaciones previstas en este artículo no serán exigibles hasta el 15 de enero de 2015.

2. El Gobierno podrá ampliar el ámbito de aplicación de este artículo a empresas o entidades que no presten al público en general servicios de especial trascendencia económica en los casos en que se considere que deban tener una interlocución telemática con sus clientes o usuarios, por la naturaleza de los servicios que prestan, y emitan un número elevado de facturas.

3. Las facturas electrónicas deberán cumplir, en todo caso, lo dispuesto en la normativa específica sobre facturación.

4. Las empresas prestadoras de servicios deberán facilitar acceso a los programas necesarios para que los usuarios puedan leer, copiar, descargar e imprimir la factura electrónica de forma gratuita sin tener que acudir a otras fuentes para proveerse de las aplicaciones necesarias para ello.

Deberán habilitar procedimientos sencillos y gratuitos para que los usuarios puedan revocar el consentimiento dado a la recepción de facturas electrónicas en cualquier momento.

5. El período durante el que el cliente puede consultar sus facturas por medios electrónicos establecido en el artículo 2.1 b) no se altera porque aquel haya resuelto su contrato con la empresa o revocado su consentimiento para recibir facturas electrónicas. Tampoco caduca por esta causa su derecho a acceder a las facturas emitidas con anterioridad.

6. Las empresas que, estando obligadas a ello, no ofrezcan a los usuarios la posibilidad de recibir facturas electrónicas o no permitan el acceso de las personas que han dejado de ser clientes, a sus facturas, serán sancionadas con apercibimiento o una multa de hasta 10.000 euros. La sanción se determinará y graduará conforme a los criterios establecidos en el artículo 33 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Idéntica sanción puede imponerse a las empresas que presten servicios al público en general de especial trascendencia económica que no cumplan las demás obligaciones previstas en el artículo 2.1.

Es competente para imponer esta sanción el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

Artículo 2 ter. *Eficacia ejecutiva de la factura electrónica.*

1. La factura electrónica podrá pagarse mediante adeudo domiciliado si se incluye en la correspondiente extensión el identificador de cuenta de pago del deudor y en un anexo, el documento que acredite el consentimiento del deudor a que se refiere la Ley 16/2009, de 13 de noviembre, de servicios de pago.

2. Las facturas electrónicas llevarán aparejada ejecución si las partes así lo acuerdan expresamente. En ese caso, su carácter de título ejecutivo deberá figurar en la factura y el acuerdo firmado entre las partes por el que el deudor acepte dotar de eficacia ejecutiva a cada factura, en un anexo. En dicho acuerdo se hará referencia a la relación subyacente que haya originado la emisión de la factura.

La falta de pago de la factura que reúna estos requisitos, acreditada fehacientemente o, en su caso, mediante la oportuna declaración emitida por la entidad domiciliaria, faculta al acreedor para instar su pago mediante el ejercicio de una acción ejecutiva de las previstas en el artículo 517 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

3. En las relaciones con consumidores y usuarios, la factura electrónica no podrá tener eficacia ejecutiva.

4. Lo dispuesto en este artículo no será aplicable al pago de las facturas que tengan por destinatarios a los órganos, organismos y entidades integrantes del sector público.

Artículo 3. *Ofertas públicas de contratación electrónica entre empresas.*

1. A los efectos de este precepto se entiende por oferta pública de contratación electrónica entre empresas, aquel servicio de la sociedad de la información que consiste en un proceso enteramente electrónico abierto y limitado en el tiempo, por el que una empresa ofrece la posibilidad de comprar o vender un determinado tipo de productos a otras empresas de manera que la contratación final se adjudique a la propuesta mejor valorada.

2. Las ofertas públicas de contratación electrónica entre empresas que se adscriban al protocolo de transparencia descrito en el apartado 3 de este artículo podrán ostentar la denominación de «Oferta pública de contratación electrónica de transparencia garantizada».

3. Para que una oferta pública de contratación electrónica entre empresas sea calificada de «Oferta pública de contratación electrónica de transparencia garantizada» deberá responder a los siguientes requisitos mínimos:

a) La empresa adjudicadora que decida recurrir a una oferta pública de contratación electrónica hará mención de ello en el anuncio de licitación que se publicará en la página corporativa de la empresa de forma accesible y visible para el conjunto de las empresas o para algunas previamente seleccionadas.

En el anuncio de licitación se invitará a presentar ofertas en un plazo razonable a partir de la fecha de publicación del anuncio.

b) Las condiciones de la empresa adjudicadora incluirán, al menos, información sobre los elementos a cuyos valores se refiere la oferta de pública de contratación electrónica, siempre que sean cuantificables y puedan ser expresados en cifras o porcentajes; en su caso, los límites de los valores que podrán presentarse, tal como resultan de las especificaciones del objeto del contrato; la información que se pondrá a disposición de los licitadores durante la oferta pública de contratación electrónica y el momento en que, en su caso, dispondrán de dicha información; la información pertinente sobre el desarrollo de la oferta pública de contratación electrónica; las condiciones en las que los licitadores podrán pujar, y, en particular, las diferencias mínimas que se exigirán, en su caso, para pujar; la información pertinente sobre el dispositivo electrónico utilizado y sobre las modalidades y especificaciones técnicas de conexión.

c) A lo largo del proceso de la oferta pública de contratación electrónica, la empresa adjudicadora comunicará a todos los licitadores como mínimo la información que les permita conocer en todo momento su respectiva clasificación. La empresa adjudicadora podrá, asimismo, comunicar otros datos relativos a otros precios o valores presentados. Los participantes únicamente podrán utilizar la información a la que se refiere este párrafo a fin de conocer su clasificación, sin que puedan proceder a su tratamiento para otra finalidad distinta de la señalada.

d) La empresa adjudicadora cerrará la oferta pública de contratación electrónica de conformidad con la fecha y hora fijadas previamente en el anuncio de licitación de la oferta pública de contratación.

e) Una vez concluido el proceso, la empresa informará a los participantes de la decisión adoptada.

4. El Gobierno promoverá que las empresas se adhieran a la calificación de «Oferta pública de contratación electrónica de transparencia garantizada» en sus relaciones comerciales.

CAPÍTULO II

Modificaciones legislativas para el impulso de la sociedad de la información y de las comunicaciones electrónicas

Artículo 4. *Modificaciones de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.*

Se modifica la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en los siguientes aspectos:

Uno. Se da nueva redacción al párrafo primero del artículo 4, con el texto siguiente:

«A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo, les será de aplicación lo dispuesto en los artículos 7.2 y 11.2.»

Dos. Se da nueva redacción al artículo 8, con el texto siguiente:

«Artículo 8. *Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.*

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

2. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

3. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo

con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

4. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

5. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.»

Tres. Se suprime el artículo 9, sobre constancia registral del nombre de dominio, que queda sin contenido.

Cuatro. Se da nueva redacción a los párrafos b) y f) del apartado 1 del artículo 10, con el texto siguiente:

«b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.»

«f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.»

Cinco. Se da nueva redacción al artículo 11, con el texto siguiente:

«Artículo 11. *Deber de colaboración de los prestadores de servicios de intermediación.*

1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes

materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.»

Seis. Se incluye un nuevo artículo 12 bis, con la siguiente redacción:

«Artículo 12 bis. *Obligaciones de información sobre seguridad.*

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.»

Siete. Se da nueva redacción al apartado 2 del artículo 17, con el texto siguiente:

«2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.»

Ocho. Se modifica el apartado 3 del artículo 18, teniendo éste el siguiente tenor literal:

«3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.»

Nueve. Se da nueva redacción al artículo 20, con el texto siguiente:

«Artículo 20. *Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra "publicidad" o la abreviatura "publi".

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo, comercio electrónico o publicidad.»

Diez. Se da nueva redacción al apartado 1 del artículo 24, con el texto siguiente:

«1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.»

Once. Se da nueva redacción a la rúbrica y a los apartados 1 y 2 del artículo 27, con el texto siguiente:

«Artículo 27. *Obligaciones previas a la contratación.*

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.

b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.

c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y

d) La lengua o lenguas en que podrá formalizarse el contrato.

La obligación de poner a disposición del destinatario la información referida en el párrafo anterior se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en dicho párrafo.

Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.»

Doce. Se da una nueva redacción al artículo 33, con el siguiente texto:

«Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de sociedad de la información, sanidad y consumo de las Administraciones Públicas, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica,

b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y

c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.»

Trece. Se da una nueva redacción a los apartados 1 y 2 del artículo 35, con el texto siguiente:

«1. El Ministerio de Industria, Turismo y Comercio en el ámbito de la Administración General del Estado, y los órganos que correspondan de las Comunidades Autónomas, controlarán, en sus respectivos ámbitos territoriales y competenciales, el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. Los órganos citados en el apartado 1 de este artículo podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos a dichos órganos y que ejerzan la inspección a que se refiere el párrafo anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.»

Catorce. Se suprime la letra a) del apartado 2 del artículo 38 que queda sin contenido.

Quince. Se da nueva redacción a la letra a) del apartado 4 del artículo 38, con el texto siguiente:

«a) El incumplimiento de lo previsto en el artículo 12 bis.»

Dieciséis. Se da una nueva redacción al artículo 43, con el siguiente texto:

«1. La imposición de sanciones por incumplimiento de lo previsto en esta Ley corresponderá al órgano o autoridad que dictó la resolución incumplida o al que estén adscritos los inspectores. Asimismo las infracciones respecto a los derechos y garantías de los consumidores y usuarios serán sancionadas por el órgano correspondiente de las Comunidades Autónomas competentes en materia de consumo.

2. En la Administración General del Estado, la imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Industria, Turismo y Comercio, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la

comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

3. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses.»

Diecisiete. Se da una nueva redacción a la disposición adicional tercera, con el texto siguiente:

«Disposición adicional tercera. *Sistema Arbitral de Consumo.*

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente que se prestará también por medios electrónicos, conforme al procedimiento establecido reglamentariamente.»

Dieciocho. Se da nueva redacción al párrafo segundo del apartado uno de la disposición adicional quinta, con el texto siguiente:

«A partir del 31 de diciembre de 2008, las páginas de Internet de las Administraciones Públicas satisfarán, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.»

Diecinueve. Se añaden dos nuevos párrafos, que pasarán a ser respectivamente el tercero y el cuarto, al apartado uno de la disposición adicional quinta, con el texto siguiente:

«Las Administraciones Públicas exigirán que tanto las páginas de Internet cuyo diseño o mantenimiento financien total o parcialmente como las páginas de Internet de entidades y empresas que se encarguen de gestionar servicios públicos apliquen los criterios de accesibilidad antes mencionados. En particular, será obligatorio lo expresado en este apartado para las páginas de Internet y sus contenidos de los Centros públicos educativos, de formación y universitarios, así como, de los Centros privados que obtengan financiación pública.

Las páginas de Internet de las Administraciones Públicas deberán ofrecer al usuario información sobre su nivel de accesibilidad y facilitar un sistema de contacto para que puedan transmitir las dificultades de acceso al contenido de las páginas de Internet o formular cualquier queja, consulta o sugerencia de mejora.»

Veinte. Se añaden tres nuevos apartados, que pasarán a ser los apartados tres, cuatro y cinco, a la disposición adicional quinta, con el texto siguiente:

«Tres. Las Administraciones Públicas promoverán medidas de sensibilización, educación y formación sobre accesibilidad con objeto de promover que los titulares de otras páginas de Internet incorporen progresivamente los criterios de accesibilidad.

Cuatro. Los incumplimientos de las obligaciones de accesibilidad establecidas en esta Disposición adicional estarán sometidos al régimen de infracciones y sanciones vigente en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Cinco. Las páginas de Internet de las empresas que presten servicios al público en general de especial trascendencia económica, sometidas a la obligación establecida en el artículo 2 de la Ley 56/2007, de medidas de impulso de la sociedad de la información, deberán satisfacer a partir del 31 de diciembre de 2008, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.»

Artículo 5. *Modificaciones de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

Se modifica la Ley 59/2003, de 19 de diciembre, de firma electrónica, en los siguientes aspectos:

Uno. Se da nueva redacción al apartado 5 del artículo 3, con el texto siguiente:

«5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.»

Dos. Se da nueva redacción al apartado 8 del artículo 3, con el texto siguiente:

«8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.»

Tres. Se da nueva redacción a los apartados 2 y 3 del artículo 13, con el texto siguiente:

«2. En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y d4e apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

3. Si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.»

Cuatro. Se da nueva redacción al apartado 5 del artículo 23, con el texto siguiente:

«5. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación podrá, en su caso, comprobarlos en el citado registro antes de la expedición del certificado, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.»

Cinco. Se da nueva redacción al apartado 4 del artículo 31, con el texto siguiente:

«4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.»

Seis. Se añade una disposición adicional, con la siguiente redacción:

«Disposición adicional undécima. *Resolución de conflictos.*

Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.

Cuando el usuario tenga la condición de consumidor o usuario, en los términos establecidos por la legislación de protección de los consumidores, el prestador y el usuario podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente.»

Artículo 6. *Modificación de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista.*

Se añade una nueva letra i) al artículo 64 de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista, con la siguiente redacción:

«i) Los incumplimientos de lo dispuesto en el párrafo d) del apartado 1 del citado artículo 2 serán sancionables conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal correspondiendo la potestad sancionadora al órgano que resulte competente.»

Artículo 7. *Modificaciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

Se modifica la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en los siguientes aspectos:

Uno. Se modifican las letras a) y c) del apartado 1 del artículo 22 quedando con la siguiente redacción:

«a) Que todos los usuarios finales puedan obtener una conexión a la red telefónica pública desde una ubicación fija y acceder a la prestación del servicio telefónico disponible al publico, siempre que sus solicitudes se consideren razonables en los términos que reglamentariamente se determinen. La conexión debe ofrecer al usuario final la posibilidad de efectuar y recibir llamadas telefónicas y

permitir comunicaciones de fax y datos a velocidad suficiente para acceder de forma funcional a Internet. No obstante, la conexión deberá permitir comunicaciones en banda ancha, en los términos que se definan por la normativa vigente.»

«c) Que exista una oferta suficiente de teléfonos públicos de pago, en todo el territorio nacional, que satisfaga razonablemente las necesidades de los usuarios finales, en cobertura geográfica, en número de aparatos, accesibilidad de estos teléfonos por los usuarios con discapacidades y calidad de los servicios y, que sea posible efectuar gratuitamente llamadas de emergencia desde los teléfonos públicos de pago sin tener que utilizar ninguna forma de pago, utilizando el número único de llamadas de emergencia 112 y otros números de emergencia españoles. Asimismo, en los términos que se definan por la normativa vigente para el servicio universal, que exista una oferta suficiente de equipos terminales de acceso a Internet de banda ancha.»

Dos. Se introduce una nueva redacción en el apartado l) del artículo 53 que queda redactado de la siguiente forma:

«l) El incumplimiento grave o reiterado de las obligaciones de servicio público y la grave o reiterada vulneración de los derechos de los consumidores y usuarios finales según lo establecido en el Título III de la Ley y su normativa de desarrollo, con excepción de los establecidos por el artículo 38.3 cuya vulneración será sancionable conforme a lo previsto en el párrafo z) de este artículo.»

Tres. El apartado o) del artículo 54 queda redactado de la siguiente forma:

«o) El incumplimiento de las obligaciones de servicio público y la vulneración de los derechos de los consumidores y usuarios finales, según lo establecido en el Título III de la Ley y su normativa de desarrollo, salvo que deban considerarse como infracción muy grave, conforme a lo previsto en el artículo anterior.

No obstante, la vulneración de los derechos establecidos por el artículo 38.3 de esta Ley será sancionable conforme a lo previsto en el párrafo r) de este artículo.»

Cuatro. Se modifica el apartado 7 del punto 3 del Anexo I, que queda redactado como sigue:

«Las Administraciones Públicas estarán exentas del pago de esta tasa en los supuestos de reserva de dominio público radioeléctrico para la prestación de servicios obligatorios de interés general que tenga exclusivamente por objeto la defensa nacional, la seguridad pública y las emergencias, así como cualesquiera otros servicios obligatorios de interés general sin contrapartida económica directa o indirecta, como tasas, precios públicos o privados, ni otros ingresos derivados de dicha prestación, tales como los ingresos en concepto de publicidad. A tal efecto, deberán solicitar, fundamentadamente, dicha exención al Ministerio de Industria, Turismo y Comercio. Asimismo, no estarán sujetos al pago los enlaces descendentes de radiodifusión por satélite, tanto sonora como de televisión.»

Cinco. Se añade un nuevo apartado 5 al epígrafe 4 «Tasas de telecomunicaciones», del Anexo I «Tasas en materia de telecomunicaciones», con la siguiente redacción:

«5. Estarán exentos del pago de la tasa de tramitación de autorizaciones de uso especial de dominio público radioeléctrico aquellos solicitantes de dichas autorizaciones que cumplan 65 años en el año en que efectúen la solicitud, o que los hayan cumplido con anterioridad, así como los beneficiarios de una pensión pública o que tengan reconocido un grado de minusvalía igual o superior al 33 por 100.»

Artículo 8. *Modificación de los apartados 9 y 10 de la Disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifican los apartados 9 y 10 de la Disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que quedarán redactados de la siguiente forma:

«9. Los recursos económicos de la entidad podrán provenir de cualquiera de los enumerados en el apartado 1 del artículo 65 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Entre los recursos económicos de la entidad pública empresarial Red.es se incluyen los ingresos provenientes de lo recaudado en concepto del precio público por las operaciones de registro relativas a los nombres de dominio de Internet bajo el código de país correspondiente a España ".es" regulado en el apartado siguiente.

10. Precios Públicos por asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el ".es".

La contraprestación pecuniaria que se satisfaga por la asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España tendrán la consideración de precio público.

Red.es, previa autorización del Ministerio de Industria, Turismo y Comercio, establecerá mediante la correspondiente Instrucción, las tarifas de los precios públicos por la asignación, renovación y otras operaciones de registro de los nombres de dominio bajo el ".es". La propuesta de establecimiento o modificación de la cuantía de precios públicos irá acompañada, de conformidad con lo previsto en el artículo 26 de la Ley 8/1989, de 13 de abril, que regula el Régimen Jurídico de las Tasas y Precios Públicos, de una memoria económico-financiera que justificará el importe de los mismos que se proponga y el grado de cobertura financiera de los costes correspondientes.

La gestión recaudatoria de los precios públicos referidos en este apartado corresponde a la entidad pública empresarial Red.es que determinará el procedimiento para su liquidación y pago mediante la Instrucción mencionada en el párrafo anterior en la que se establecerán los modelos de declaración, plazos y formas de pago.

La entidad pública empresarial Red.es podrá exigir la anticipación o el depósito previo del importe total o parcial de los precios públicos por las operaciones de registro relativas a los nombres de dominio ".es".»

Disposición adicional primera. *Utilización de caracteres de las lenguas oficiales de España en el «.es».*

La autoridad de asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España («.es») adoptará las medidas que sean necesarias para asegurar que puedan asignarse nombres de dominio que contengan caracteres propios de las lenguas oficiales de España distintos de los incluidos en el alfabeto inglés en un plazo máximo de 3 meses desde la entrada en vigor de esta Ley.

Con carácter previo a que los mecanismos de reconocimiento de caracteres multilingües estén disponibles para la asignación de nombres de dominio bajo el código de país «.es», la autoridad de asignación dará publicidad a la posibilidad de solicitar nombres de dominio que contengan dichos caracteres y establecerá con antelación suficiente un registro escalonado para los mismos. En este registro escalonado se dará preferencia a las solicitudes de nombres de dominio con caracteres multilingües que resulten equivalentes a nombres de dominio bajo el código de país «.es» previamente asignados, en los términos que determine la autoridad de asignación.

Disposición adicional segunda. *Extensión de servicios de acceso a banda ancha.*

El Gobierno, en colaboración con las Comunidades Autónomas, impulsará la extensión de la banda ancha con el fin de conseguir, antes del 31 de diciembre de 2008, una cobertura de servicio universal de conexión a banda ancha, para todos los ciudadanos, independientemente del tipo de tecnología utilizada en cada caso y de su ubicación geográfica.

El Gobierno analizará de manera continua y permanente las diferentes opciones tecnológicas y las condiciones de provisión de servicios de acceso a Internet de banda ancha para el conjunto de ciudadanos y empresas en España. En particular, se colaborará

con los diferentes sectores relevantes interesados, a fin de que asesoren al Gobierno en la elaboración de un informe anual sobre la situación del uso de los servicios de acceso a Internet de banda ancha en España. Este informe será de carácter público y podrá elaborar recomendaciones para acelerar el despliegue de los citados servicios.

A efectos de realizar los análisis e informes mencionados en los párrafos anteriores el Ministerio de Industria, Turismo y Comercio podrá realizar los requerimientos de información generales o particularizados que sean necesarios en los términos previstos en la disposición adicional quinta de esta Ley.

Los análisis e informes mencionados deberán realizarse de forma territorializada por Comunidades Autónomas y se compartirán los datos en formato electrónico con las Administraciones que lo soliciten.

Disposición adicional tercera. *Plan de mejora de los niveles de seguridad y confianza en Internet.*

El Gobierno elaborará, en un plazo de seis meses, un Plan, tecnológicamente neutro, para la mejora de los niveles de seguridad y confianza en Internet, que incluirá directrices y medidas para aumentar la seguridad frente a las amenazas de Internet y proteger la privacidad on line. Este plan se revisará periódicamente para poder responder al escenario de amenazas en continua evolución.

Disposición adicional cuarta. *Requerimientos de información para fines estadísticos y de análisis.*

1. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, y los órganos estadísticos de las Comunidades Autónomas con competencias en materia de estadística, podrán requerir de los fabricantes de productos y proveedores de servicios referentes a las Tecnologías de la Información, a la Sociedad de la Información, a los contenidos digitales y al entretenimiento digital la información necesaria para el ejercicio de sus funciones para fines estadísticos y de análisis.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá dictar circulares que deberán ser publicadas en el Boletín Oficial del Estado, en las cuales se expondrá de forma detallada y concreta el contenido de la información que se vaya a solicitar, especificando de manera justificada la función para cuyo desarrollo es precisa tal información y el uso que pretende hacerse de la misma.

No obstante lo señalado en el párrafo precedente, el Ministerio de Industria, Turismo y Comercio podrá en todo caso realizar requerimientos de información particularizados sin necesidad de que previamente se dicte una circular de carácter general.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá realizar las inspecciones que considere necesarias con el fin de confirmar la veracidad de la información que en cumplimiento de los citados requerimientos le sea aportada.

Los datos e informaciones obtenidos por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en el desempeño de sus funciones, que tengan carácter confidencial por tratarse de materias protegidas por el secreto comercial, industrial o estadístico, sólo podrán ser cedidos a la Administración General del Estado y a las Comunidades Autónomas en el ámbito de sus competencias. El personal de dichas Administraciones Públicas que tenga conocimiento de estos datos estará obligado a mantener el debido secreto y sigilo respecto de los mismos.

Las entidades que deben suministrar esos datos e informaciones podrán indicar, de forma justificada, qué parte de los mismos consideran de trascendencia comercial o industrial, cuya difusión podría perjudicarles, a los efectos de que sea declarada su confidencialidad respecto de cualesquiera personas o entidades que no sean la propia Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, la Administración General del Estado o las Comunidades Autónomas, previa la oportuna justificación. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información decidirá, de forma motivada, sobre la información que, según la legislación vigente, esté exceptuada del secreto comercial o industrial y sobre la amparada por la confidencialidad.

2. Son infracciones de la obligación de cumplir los requerimientos de información establecida en el apartado anterior las conductas que se tipifican en los apartados siguientes.

Las infracciones establecidas en la presente disposición adicional se entenderán sin perjuicio de las responsabilidades civiles, penales o de otro orden en que puedan incurrir los titulares de las entidades que desarrollan las actividades a que se refieren.

3. Las infracciones administrativas tipificadas en los apartados siguientes se clasifican en muy graves, graves y leves.

4. Son infracciones muy graves:

a) La negativa reiterada a facilitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información la información que se reclame de acuerdo con lo previsto en la presente Ley.

b) Facilitar intencionadamente a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información datos falsos.

5. Son infracciones graves:

La negativa expresa a facilitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información la información que se reclame de acuerdo con lo previsto en la presente Ley.

6. Son infracciones leves:

No facilitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información los datos requeridos o retrasar injustificadamente su aportación cuando resulte exigible.

7. Por la comisión de las infracciones señaladas en los apartados anteriores, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves tipificadas en el apartado 4, multa desde 25.000 euros hasta 50.000 euros.

b) Por la comisión de infracciones graves tipificadas en el apartado 5, multa desde 5.000 euros hasta 25.000 euros.

c) Por la comisión de infracciones leves tipificadas en el apartado 6, multa de hasta 5.000 euros.

En todo caso, la cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

d) El daño causado.

Las sanciones impuestas por infracciones muy graves podrán ser publicadas en el «Boletín Oficial del Estado» una vez que la resolución sancionadora tenga carácter firme.

8. La competencia para la imposición de las sanciones muy graves corresponderá al Ministro de Industria, Turismo y Comercio y la imposición de sanciones graves y leves al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las Administraciones Públicas.

9. Las estadísticas públicas que elabore la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información relativas a personas físicas ofrecerán sus datos desagregados por sexo, considerando, si ello resultase conveniente, otras variables relacionadas con el sexo para facilitar la evaluación del impacto de género y la mejora en la efectividad del principio de igualdad entre mujeres y hombres.

10. En caso de que la información recabada en ejercicio de las funciones establecidas en esta disposición adicional contuviera datos de carácter personal será de aplicación lo

dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en su normativa de desarrollo.

Disposición adicional quinta. *Canalizaciones para el despliegue de redes de comunicaciones electrónicas en carreteras e infraestructuras ferroviarias de competencia estatal.*

1. Los proyectos de obras de construcción de nuevas carreteras o de nuevas líneas de ferrocarril que vayan a formar parte de las redes de interés general deberán prever, de acuerdo con lo que se determine reglamentariamente, la instalación de canalizaciones que permitan el despliegue a lo largo de las mismas de redes de comunicaciones electrónicas. Dichas canalizaciones deberán ponerse a disposición de los operadores de redes y servicios de comunicaciones electrónicas interesados en condiciones equitativas, no discriminatorias, neutrales y orientadas a costes.

Las condiciones de acceso se negociarán de mutuo acuerdo entre las partes. A falta de acuerdo, estas condiciones se establecerán mediante resolución de la Comisión del Mercado de las Telecomunicaciones.

En las mismas condiciones deberá preverse igualmente la facilitación de instalaciones para asegurar la cobertura de comunicaciones móviles en todo el recorrido, incluyendo los terrenos para la instalación de estaciones base, espacios para la instalación de los repetidores o dispositivos radiantes necesarios para garantizar la cobertura en túneles y el acceso a fuentes de energía eléctrica.

2. Sin perjuicio de la notificación a la que se refiere el artículo 6 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los organismos públicos responsables de la administración de las carreteras y líneas de ferrocarril de competencia estatal y las sociedades estatales que tengan encomendada su explotación podrán explotar las canalizaciones o establecer y explotar las redes de telecomunicaciones que discurran por las citadas infraestructuras de transporte en los términos previstos en la citada Ley General de Telecomunicaciones, garantizando el acceso de los restantes operadores públicos y privados a las mismas en condiciones de igualdad y neutralidad.

3. Los Ministros de Fomento y de Industria, Turismo y Comercio desarrollarán conjuntamente, en un plazo no superior a seis meses, lo establecido en esta disposición y determinarán los supuestos en que, en función del itinerario, la dimensión y demás circunstancias específicas de las nuevas carreteras o de las nuevas líneas de ferrocarril, los proyectos de obras de construcción deberán prever las canalizaciones o instalaciones a que se refiere el apartado primero.

Disposición adicional sexta. *Base de datos sobre servicios de la sociedad de la información y servicios de comunicaciones electrónicas en España.*

Con el fin de mejorar el diseño, ejecución y seguimiento de políticas relativas a la sociedad de la información, el Ministerio de Industria, Turismo y Comercio elaborará, en colaboración con las Comunidades Autónomas, una base de datos actualizada sobre los servicios de la sociedad de la información y servicios de comunicaciones electrónicas en España. Esta base de datos será sectorizada como mínimo por ámbitos territoriales de Comunidad Autónoma y los datos serán compartidos con las Administraciones que lo soliciten.

A los efectos de lo dispuesto en el párrafo anterior, el Ministerio de Industria, Turismo y Comercio podrá realizar los requerimientos de información generales o particularizados que sean necesarios en los términos previstos en la disposición adicional quinta de esta Ley.

El contenido y alcance de la base de datos referida en el párrafo primero de esta disposición adicional serán regulados mediante Orden del Ministro de Industria, Turismo y Comercio.

En lo que respecta a servicios de la sociedad de la información relativos a administración electrónica corresponderá al Ministerio de Administraciones Públicas, en colaboración con el Ministerio de Industria, Turismo y Comercio y con las Comunidades Autónomas, la regulación, elaboración y mantenimiento del correspondiente catálogo.

Disposición adicional séptima. *Agencia Estatal de Radiocomunicaciones.*

Se da nueva redacción al apartado 13 del artículo 47 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que queda redactado de la siguiente forma:

> «La constitución efectiva de la Agencia tendrá lugar en el momento y con los plazos que señale el Real Decreto de aprobación de su Estatuto. En el citado real decreto se determinarán los órganos y servicios en que se estructurará la Agencia.»

Disposición adicional octava. *Sede de la Comisión del Mercado de las Telecomunicaciones.*

Se modifica el apartado 13 del artículo 48 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que queda redactado en los siguientes términos:

> «13. La Comisión tendrá su sede en Barcelona y dispondrá de su propio patrimonio, independiente del patrimonio del Estado.»

Disposición adicional novena. *Modificación de la Ley 2/1995, de 23 de marzo, de Sociedades de Responsabilidad Limitada.*

Se introduce una nueva disposición final, con la siguiente redacción:

> **«Disposición final tercera.** *Bolsa de denominaciones sociales, estatutos orientativos y plazo reducido de inscripción.*
>
> 1. Se autoriza al Gobierno para regular una Bolsa de Denominaciones Sociales con reserva.
> 2. Por Orden del Ministro de Justicia podrá aprobarse un modelo orientativo de estatutos para la sociedad de responsabilidad limitada.
> 3. Si la escritura de constitución de una sociedad de responsabilidad limitada contuviese íntegramente los estatutos orientativos a que hace referencia el apartado anterior, y no se efectuaran aportaciones no dinerarias, el registrador mercantil deberá inscribirla en el plazo máximo de cuarenta y ocho horas, salvo que no hubiera satisfecho el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados en los términos previstos en la normativa reguladora del mismo.»

Disposición adicional décima. *Modificación del texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre.*

Se modifica el apartado segundo del artículo 15 del texto refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre, con el texto siguiente:

> «No obstante, si la fecha de comienzo de las operaciones sociales coincide con la de otorgamiento de la escritura fundacional, y salvo que los estatutos sociales o la escritura dispongan otra cosa, se entenderá que los administradores ya quedan facultados para el pleno desarrollo del objeto social y para realizar toda clase de actos y contratos, de los que responderán la sociedad en formación y los socios en los términos que se han indicado.»

Disposición adicional undécima. *Acceso de las personas con discapacidad a las tecnologías de la Sociedad de la Información.*

Las Administraciones Públicas, en el ámbito de sus respectivas competencias, promoverán el impulso, el desarrollo y la aplicación de los estándares de accesibilidad para personas con discapacidad y diseño para todos, en todos los elementos y procesos basados en las nuevas tecnologías de la Sociedad de la Información.

Disposición adicional duodécima. *Lenguas Oficiales.*

Las Administraciones Públicas deberán fomentar el pluralismo lingüístico en la utilización de las nuevas tecnologías de la Sociedad de la Información, en particular en los ámbitos territoriales en que existan lenguas propias.

Disposición adicional decimotercera. *Regulación de los instrumentos telemáticos utilizados por los profesionales que elaboren proyectos e informes incorporados a procedimientos tramitados por las Administraciones.*

Las Administraciones Públicas regularán los instrumentos telemáticos necesarios para ser utilizados por los profesionales debidamente colegiados que elaboren y preparen proyectos e informes que deben incorporarse preceptivamente en los procedimientos que tramiten los órganos administrativos.

Disposición adicional decimocuarta. *Transferencia tecnológica a la sociedad.*

El Centro Nacional de Referencia de Aplicación de las Tecnologías de Información y Comunicación (CENATIC), en colaboración con los centros autonómicos de referencia y con el Centro de Transferencia de Tecnología entre Administraciones Públicas de la Administración General del Estado, se encargara de la puesta en valor y difusión entre entidades privadas y la ciudadanía en general, de todas aquellas aplicaciones que sean declaradas de fuentes abiertas por las administraciones públicas, haciendo llegar a los autores o comunidades de desarrollo cualquier mejora o aportación que sea realizada sobre las mismas.

Asimismo, el CENATIC se encargará del asesoramiento general sobre los aspectos jurídicos, tecnológicos y metodológicos más adecuados para la liberación del software y conocimiento.

Disposición adicional decimoquinta. *Fomento a la participación ciudadana en la sociedad de la información.*

Con el objeto de fomentar la presencia de la ciudadanía y de las entidades privadas sin ánimo de lucro y garantizar el pluralismo, la libertad de expresión y la participación ciudadana en la sociedad de la información, se establecerán medios de apoyo y líneas de financiación para el desarrollo de servicios de la sociedad de la información sin finalidad lucrativa que, promovidos por entidades ciudadanas, fomenten los valores democráticos y la participación ciudadana, atiendan al interés general o presten servicio a comunidades y grupos sociales desfavorecidos.

Disposición adicional decimosexta. *Contenidos digitales de titularidad pública para su puesta a disposición de la sociedad.*

Siempre que por su naturaleza no perjudique al normal funcionamiento de la Administración, ni afecte al interés público o al interés general, los contenidos digitales o digitalizados de que dispongan las Administraciones Públicas, cuyos derechos de propiedad intelectual le pertenezcan sin restricciones o sean de dominio público, serán puestos a disposición del público, en los términos legalmente establecidos, de forma telemática sin restricciones tecnológicas, para su uso consistente en el estudio, copia o redistribución, siempre que las obras utilizadas de acuerdo con lo anteriormente señalado citen al autor y se distribuyan en los mismos términos.

Disposición adicional decimoséptima. *Cesión de contenidos para su puesta a disposición de la sociedad.*

Las personas físicas o jurídicas podrán ceder sus derechos de explotación sobre obras para que una copia digitalizada de las mismas pueda ser puesta a disposición del público de forma telemática, sin restricciones tecnológicas o metodológicas, y libres para ser usado con cualquier propósito, estudiados, copiados, modificados y redistribuidos, siempre que las obras derivadas se distribuyan en los mismos términos.

Disposición adicional decimoctava. *Televisión de proximidad sin ánimo de lucro.*

1. El Ministerio de Industria, Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, mediante Resolución del Secretario de Estado, planificará frecuencias para la gestión indirecta del servicio de televisión local de proximidad por parte de entidades sin ánimo de lucro que se encontraran habilitadas para emitir al amparo de la Disposición Transitoria Primera de la Ley 41/1995, de 22 de diciembre, de Televisión Local por Ondas Terrestres, siempre que se disponga de frecuencias para ello.

Tienen la consideración de servicios de difusión de televisión de proximidad aquellos sin finalidad comercial que, utilizando las frecuencias que en razón de su uso por servicios próximos no estén disponibles para servicios de difusión de televisión comercialmente viables, están dirigidos a comunidades en razón de un interés cultural, educativo, étnico o social.

El canal de televisión difundido lo será siempre en abierto. Su programación consistirá en contenidos originales vinculados con la zona y comunidad a la que vayan dirigidos y no podrá incluir publicidad ni televenta, si bien se admitirá el patrocinio de sus programas.

La entidad responsable del servicio de televisión local de proximidad no podrá ser titular directa o indirectamente de ninguna concesión de televisión de cualquier cobertura otorgada por la Administración que corresponda.

2. Corresponde al Gobierno aprobar el reglamento general de prestación del servicio, con carácter de norma básica, y el reglamento técnico, en el que se establezca el procedimiento para la planificación de las frecuencias destinadas a servicios de difusión de televisión de proximidad, atendiendo entre otros extremos a las necesidades de cobertura, población y características propias de este servicio.

Dicho reglamento establecerá las condiciones técnicas que deberán reunir las frecuencias destinadas a estos servicios, la extensión máxima de la zona de servicio, la determinación concreta de las potencias de emisión, características y uso compartido del múltiplex asignado para la prestación del servicio y el procedimiento por el que las Comunidades Autónomas solicitarán la reserva de frecuencias para estos servicios, así como el procedimiento de asignación por parte de la Agencia Estatal de Radiocomunicaciones.

La planificación del espectro para la televisión de proximidad no será prioritaria con respecto a otros servicios planificados o planificables.

3. Será de aplicación a estas televisiones lo dispuesto en la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, sobre la coordinación de disposiciones legales, reglamentarias y administrativas de los Estados miembros, relativas al ejercicio de actividades de radiodifusión televisiva, y lo previsto en los artículos 1, 2, 6, apartados 2 y 3 del artículo 9, 10, 11, 15, 18, 20, 21, 22 y apartado 4 de la disposición transitoria segunda de la Ley 41/1995, de 22 de diciembre, de Televisión Local por Ondas Terrestres. Igualmente les será de aplicación lo dispuesto en la Disposición Adicional Trigésima de la Ley 62/2003, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social.

4. Las Comunidades Autónomas adjudicarán las correspondientes concesiones para la prestación de servicios de televisión de proximidad, de acuerdo con el reglamento general de prestación del servicio y su normativa.

5. Las concesiones para la prestación de servicios de difusión de radio y televisión de proximidad se otorgarán por un plazo de cinco años y podrán ser renovadas hasta en tres ocasiones, siempre que su actividad no perjudique la recepción de los servicios de difusión legalmente habilitados que coincidan total o parcialmente con su zona de cobertura.

Estas concesiones obligan a la explotación directa del servicio y serán intransferibles.

6. Las concesiones para la prestación de servicios de televisión de proximidad se extinguirán, además de por alguna de las causas generales previstas en el artículo 15 de la Ley 41/1995, de 22 de diciembre, de Televisión Local por Ondas Terrestres, por extinción de la personalidad jurídica de su titular y por su revocación.

7. Serán causas de revocación de la concesión la utilización de las mismas para la difusión de servicios comerciales y la modificación de las condiciones de planificación del espectro radioeléctrico sin que exista una frecuencia alternativa.

Disposición adicional decimonovena. *Modificación de la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores y de la Ley 36/2007, de 16 de noviembre, por la que se modifica la Ley 13/1985, de 25 de mayo, de coeficientes de inversión, recursos propios y obligaciones de información de los intermediarios financieros y otras normas del sistema financiero.*

1. Se modifica la letra b) de la Disposición Derogatoria de la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores, que tendrá la siguiente redacción:

> «b) El párrafo segundo del apartado 1 del artículo 83.a) de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro.»

2. Se modifican los apartados 2, 3 y 4 de la Disposición transitoria primera de la Ley 36/2007, de 16 de noviembre, por la que se modifica la Ley 13/1985, de 25 de mayo, de coeficientes de inversión, recursos propios y obligaciones de información de los intermediarios financieros y otras normas del sistema financiero, que tendrán la siguiente redacción:

> «2. Durante el primer y segundo período de doce meses posteriores al 31 de diciembre de 2007, las entidades de crédito o los grupos consolidables de entidades de crédito que utilicen los métodos internos de medición de riesgo operacional mantendrán recursos propios que serán en todo momento iguales o superiores a los importes indicados en los apartados 3 y 4.
> 3. Para el primer período de doce meses previsto en el apartado 1 y en el apartado 2, el importe de los recursos propios será el 90 por ciento del importe total de los recursos propios mínimos que serían exigibles a la entidad o grupo de mantenerse la regulación vigente a 31 de diciembre de 2007.
> 4. Para el segundo período de doce meses contemplado en el apartado 1 y en el apartado 2, el importe de los recursos propios será el 80 por ciento del importe total de los recursos propios mínimos que serían exigibles a la entidad o grupo de mantenerse la regulación vigente a 31 de diciembre de 2007.»

Disposición adicional vigésima. *Regulación del juego.*

El Gobierno presentará un Proyecto de Ley para regular las actividades de juego y apuestas, en particular las realizadas a través de sistemas interactivos basados en comunicaciones electrónicas, que atenderá a los siguientes principios:

1. Asegurar la compatibilidad de la nueva regulación con la normativa aplicable a otros ámbitos vinculados a la prestación de este tipo de servicios, y, en especial, a la normativa de protección de los menores, de la juventud, de grupos especialmente sensibles de usuarios así como de los consumidores en general, además del ámbito de protección de datos de carácter personal y de servicios de la Sociedad de la Información.

2. Establecer una regulación sobre la explotación de actividades de juego por sistemas interactivos de acuerdo con la normativa y los principios generales del derecho comunitario.

3. Articular un sistema de control sobre los servicios de juego y apuestas por sistemas interactivos que garantice unas condiciones de mercado plenamente seguras y equitativas para los operadores de tales sistemas así como unos adecuados niveles de protección de los usuarios. En particular, deberá regular la actividad de aquellos operadores que ya cuenten con una autorización para la presentación de los mencionados servicios otorgada por las autoridades de cualquiera de los Estados miembros de la Unión Europea.

4. Establecer un sistema de tributación sobre los servicios de juego y apuestas por sistemas interactivos atendiendo al origen de las operaciones objeto de tributación. La regulación deberá igualmente prever un sistema de distribución de la tributación obtenida como consecuencia de la explotación de servicios de juego y apuestas por medios electrónicos en España entre la Administración Estatal y las Comunidades Autónomas, teniendo en cuenta la especificidad fiscal de los regímenes forales.

5. La actividad de juego y apuestas a través de sistemas interactivos basados en comunicaciones electrónicas sólo podrá ejercerse por aquellos operadores autorizados para ello por la Administración Pública competente, mediante la concesión de una autorización

tras el cumplimiento de las condiciones y requisitos que se establezcan. Quien no disponga de esta autorización no podrá realizar actividad alguna relacionada con los juegos y apuestas interactivos. En particular, se establecerán las medidas necesarias para impedir la realización de publicidad por cualquier medio así como la prohibición de utilizar cualquier medio de pago existente en España. Por otra parte, se sancionará de conformidad con la legislación de represión del contrabando la realización de actividades de juego y apuestas a través de sistemas interactivos sin contar con la autorización pertinente.

6. La competencia para la ordenación de las actividades de juegos y apuestas realizadas a través de sistemas interactivos corresponderá a la Administración General del Estado cuando su ámbito sea el conjunto del territorio nacional o abarque más de una Comunidad Autónoma.

Disposición transitoria única. *Régimen transitorio relativo a las tarifas aplicables por la asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el «.es».*

Hasta que se fijen, de conformidad con lo que se establece en el artículo 8 de esta Ley, los precios públicos aplicables por la asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el «.es» seguirán siendo de aplicación las tasas correspondientes fijadas de acuerdo con las normas legales y disposiciones reglamentarias de desarrollo vigentes con anterioridad a la entrada en vigor de esta Ley.

Disposición final primera. *Fundamento constitucional.*

1. Tienen el carácter de legislación básica los siguientes preceptos de esta Ley:

a) Los apartados 2, 3 y 5 del artículo 1 y los artículos 2 y 6, que se dictan al amparo de lo dispuesto en el apartado 13.º del artículo 149.1 de la Constitución.

b) Los apartados 1 y 4 del artículo 1, la disposición adicional duodécima y la disposición adicional decimotercera, que se dictan al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución.

c) La disposición adicional undécima, que se dicta al amparo de lo dispuesto en el artículo 149.1.1.ª y 18.ª de la Constitución.

d) La disposición adicional decimoquinta, que se dicta al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución.

2. Los artículos 3, 4 y 5 de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1. 6.ª, 8.ª y 21.ª de la Constitución, sin perjuicio de las competencias que ostenten las Comunidades Autónomas.

3. Los artículos 7 y 8 y las disposiciones adicionales primera, segunda, tercera, cuarta, quinta, sexta, séptima, octava y decimocuarta de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1.21.ª de la Constitución.

4. Las disposiciones adicionales novena y décima de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1.6.ª y 8.ª de la Constitución.

5. Las disposiciones adicionales decimosexta y decimoséptima de esta Ley se dictan al amparo de lo dispuesto en el artículo 149.1.9.ª de la Constitución.

Disposición final segunda. *Modificación de leyes por las que se incorpora derecho comunitario.*

Mediante esta Ley se modifica la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica que incorporaron respectivamente la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, y la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Disposición final tercera. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar mediante Reglamento lo previsto en esta Ley, en el ámbito de sus competencias.

Disposición final cuarta. *Entrada en vigor.*

Esta Ley entrará en vigor al día siguiente de su publicación en el Boletín Oficial del Estado.

No obstante, las obligaciones contenidas en el nuevo artículo 12 bis de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico entrarán en vigor a los tres meses de la publicación de la Ley en el Boletín Oficial del Estado, y los artículos 2 y 6 de esta Ley entrarán en vigor a los doce meses de la publicación de la Ley en el Boletín Oficial del Estado.

§ 14

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

Jefatura del Estado
«BOE» núm. 115, de 14 de mayo de 1982
Última modificación: 23 de junio de 2010
Referencia: BOE-A-1982-11196

DON JUAN CARLOS I, REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica:

Conforme al artículo dieciocho, uno, de la Constitución, los derechos al honor, a la intimidad personal y familiar y a la propia imagen tienen el rango de fundamentales, y hasta tal punto aparecen realzados en el texto constitucional que el artículo veinte, cuatro, dispone que el respeto de tales derechos constituya un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales.

El desarrollo mediante la correspondiente Ley Orgánica, a tenor del artículo ochenta y uno, uno, de la Constitución, del principio general de garantía de tales derechos contenidos en el citado artículo dieciocho, uno, de la misma constituye la finalidad de la presente ley.

Establece el artículo primero de la misma la protección civil de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen frente a todos género de injerencia o intromisiones ilegítimas. Pero no puede ignorar que algunos de esos derechos gozan o previsiblemente gozarán de una protección penal. Así ocurre con el derecho al honor, amparado por las prescripciones contenidas en el libro II, título X, del vigente Código Penal, y con determinados aspectos del derecho a la intimidad personal y familiar que son objeto de una protección de esa naturaleza en el proyecto de nuevo Código Penal recientemente aprobado por el Consejo de Ministros.

Por ello en los casos que exista la protección penal tendrá ésta preferente aplicación, por ser sin duda la de más fuerte efectividad, si bien la responsabilidad civil derivada del delito se deberá fijar de acuerdo con los criterios que esta ley establece.

Los derechos garantizados por la ley han sido encuadrados por la doctrina jurídica más autorizada entre los derechos de la personalidad, calificación de la que obviamente se desprende el carácter de irrenunciable irrenunciabilidad referida con carácter genérico a la protección civil que la ley establece.

En el artículo segundo se regula el ámbito de protección de los derechos a que se refiere. Además de la delimitación que pueda resultar de las leyes, se estima razonable admitir que en lo no previsto por ellas la esfera del honor, de la intimidad personal y familiar y del uso de la imagen esté determinada de manera decisiva por las ideas que prevalezcan en

cada momento en la Sociedad y por el propio concepto que cada persona según sus actos propios mantenga al respecto y determine sus pautas de comportamiento. De esta forma la cuestión se resuelve en la ley en términos que permiten al juzgador la prudente determinación de la esfera de protección en función de datos variables según los tiempos y las personas.

Los derechos protegidos en la ley no pueden considerarse absolutamente ilimitados. En primer lugar, los imperativos del interés público pueden hacer que por ley se autoricen expresamente determinadas entradas en el ámbito de la intimidad, que no podrán ser reputadas legítimas. De otro lado, tampoco tendrán este carácter las consentidas por el propio interesado, posibilidad ésta que no se opone a la irrenunciabilidad abstracta de dichos derechos pues ese consentimiento no implica la absoluta abdicación de los mismos sino tan sólo el parcial desprendimiento de alguna de las facultades que los integran. Ahora bien, la ley exige que el consentimiento sea expreso, y dada la índole particular de estos derechos permite que pueda ser revocado en cualquier momento, aunque con indemnización de los perjuicios que de la revocación se siguieren al destinatario del mismo. El otorgamiento del consentimiento cuando se trate de menores o incapacitados es objeto de las prescripciones contenidas en el artículo tercero.

En los artículos cuarto al sexto de la ley se contempla el supuesto de fallecimiento del titular del derecho lesionado. Las consecuencias del mismo en orden a la protección de estos derechos se determinan según el momento en que la lesión se produjo. Aunque la muerte del sujeto de derecho extingue los derechos de la personalidad la memoria de aquél constituye una prolongación de esta última que debe también ser tutelada por el Derecho, por ello, se atribuye la protección en el caso de que la lesión se hubiera producido después del fallecimiento de una persona a quien ésta hubiera designado en su testamento, en defecto de ella a los parientes supervivientes, y en último término, al Ministerio Fiscal con una limitación temporal que se ha estimado prudente. En el caso de que la lesión tenga lugar antes del fallecimiento sin que el titular del derecho lesionado ejerciera las acciones reconocidas en la ley, sólo subsistirán éstas si no hubieran podido ser ejercitadas por aquél o por su representante legal, pues si se pudo ejercitarlas y no se hizo existe una fundada presunción de que los actos que objetivamente pudieran constituir lesiones no merecieron esa consideración a los ojos del perjudicado o su representante legal. En cambio, la acción ya entablada sí será transmisible porque en este caso existe una expectativa de derecho a la indemnización.

La definición de las intromisiones o injerencias ilegítimas en el ámbito protegido se lleva a cabo en los artículos séptimo y octavo de la ley. El primero de ellos recoge en términos de razonable amplitud diversos supuestos de intromisión o injerencia que pueden darse en la vida real y coinciden con los previstos en las legislaciones protectoras existentes en otros países de desarrollo social y tecnológico igual o superior al nuestro. No obstante, existen casos en que tales injerencias o intromisiones no pueden considerarse ilegítimas en virtud de razones de interés público que imponen una limitación de los derechos individuales, como son los indicados en el artículo octavo de la ley.

Por último, la ley fija, en su artículo noveno, de acuerdo con lo prevenido en el artículo cincuenta y tres, dos, de la Constitución, el cauce legal para la defensa frente a las injerencias o intromisiones ilegítimas, así como las pretensiones que podrá deducir el perjudicado. En lo que respecta a la indemnización de perjuicios, se presume que éstos existen en todo caso de injerencias o intromisiones acreditadas, y comprenderán no sólo la de los perjuicios materiales, sino también la de los morales, de especial relevancia en este tipo de actos ilícitos. En tanto no sea regulado el amparo judicial, se considera de aplicación al efecto la Ley de Protección Jurisdiccional de los derechos de la persona de veintiséis de diciembre de mil novecientos setenta y ocho, a cuyo ámbito de protección han quedado incorporados los derechos al honor, a la intimidad personal y familiar y a la propia imagen por la disposición transitoria segunda, dos, de la Ley Orgánica dos/mil novecientos setenta y nueve, de tres de octubre, del Tribunal Constitucional.

CAPITULO I

Disposiciones generales

Artículo primero.

1. El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente Ley Orgánica.

2. El carácter delictivo de la intromisión no impedirá el recurso al procedimiento de tutela judicial previsto en el artículo 9.º de esta Ley. En cualquier caso, serán aplicables los criterios de esta Ley para la determinación de la responsabilidad civil derivada de delito.

3. El derecho al honor, a la intimidad personal y familiar y a la propia imagen es errenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de esta ley.

Artículo segundo.

Uno. La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia.

Dos. No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso **o, por imperativo del artículo 71 de la Constitución, cuando se trate de opiniones manifestadas por Diputados o Senadores en el ejercicio de sus funciones. Iniciado un proceso civil en aplicación de la presente Ley, no podrá seguirse contra un Diputado o Senador sin la previa autorización del Congreso de los Diputados o del Senado.**

La previa autorización será tramitada por el procedimiento previsto para los suplicatorios.

> Declarada la inconstitucionalidad y nulidad del inciso destacado del apartado 2 por Sentencia del TC 9/1990 de 18 de enero. Ref. BOE-T-1990-3964.

Tres. El consentimiento a que se refiere el párrafo anterior será revocable en cualquier momento, pero habrán de indemnizarse en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas.

Artículo tercero.

Uno. El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil.

Dos. En los restantes casos, el consentimiento habrá de otorgarse mediante escrito por su representante legal, quien estará obligado a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado. Si en el plazo de ocho días el Ministerio Fiscal se opusiere, resolverá el Juez.

Artículo cuarto.

Uno. El ejercicio de las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida corresponde a quien ésta haya designado a tal efecto en su testamento. La designación puede recaer en una persona jurídica.

Dos. No existiendo designación o habiendo fallecido la persona designada, estarán legitimados para recabar la protección el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento.

Tres. A falta de todos ellos, el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal, que podrá actuar de oficio a instancia de persona interesada, siempre que

no hubieren transcurrido más de ochenta años desde el fallecimiento del afectado. El mismo plazo se observará cuando el ejercicio de las acciones mencionadas corresponda a una persona jurídica designada en testamento.

Cuatro. En los supuestos de intromisión ilegítima en los derechos de las víctimas de un delito a que se refiere el apartado ocho del artículo séptimo, estará legitimado para ejercer las acciones de protección el ofendido o perjudicado por el delito cometido, haya o no ejercido la acción penal o civil en el proceso penal precedente. También estará legitimado en todo caso el Ministerio Fiscal. En los supuestos de fallecimiento, se estará a lo dispuesto en los apartados anteriores.

Artículo quinto.

Uno. Cuando sobrevivan varios parientes de los señalados en el artículo anterior, cualquiera de ellos podrá ejercer las acciones previstas para la protección de los derechos del fallecido.

Dos. La misma regla se aplicará, salvo disposición en contrario del fallecido, cuando hayan sido varias las personas designadas en su testamento.

Artículo sexto.

Uno. Cuando el titular del derecho lesionado fallezca sin haber podido ejercitar por sí o por su representante legal las acciones previstas en esta ley, por las circunstancias en que la lesión se produjo, las referidas acciones podrán ejercitarse por las personas señaladas en el artículo cuarto.

Dos. Las mismas personas podrán continuar la acción ya entablada por el titular del derecho lesionado cuando falleciere.

CAPITULO II

De la protección civil del honor, de la intimidad y de la propia imagen

Artículo séptimo.

Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.
2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.
3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.
5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos.
6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.
8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas.

Artículo octavo.

Uno. No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante.

Dos. En particular, el derecho a la propia imagen no impedirá:

a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.

b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.

c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

Artículo noveno.

Uno. La tutela judicial frente a las intromisiones ilegítimas en los derechos a que se refiere la presente Ley podrá recabarse por las vías procesales ordinarias o por el procedimiento previsto en el artículo 53.2 de la Constitución. También podrá acudirse, cuando proceda, al recurso de amparo ante el Tribunal Constitucional.

Dos. La tutela judicial comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y, en particular, las necesarias para:

a) El restablecimiento del perjudicado en el pleno disfrute de sus derechos, con la declaración de la intromisión sufrida, el cese inmediato de la misma y la reposición del estado anterior. En caso de intromisión en el derecho al honor, el restablecimiento del derecho violado incluirá, sin perjuicio del derecho de réplica por el procedimiento legalmente previsto, la publicación total o parcial de la sentencia condenatoria a costa del condenado con al menos la misma difusión pública que tuvo la intromisión sufrida.

b) Prevenir intromisiones inminentes o ulteriores.

c) La indemnización de los daños y perjuicios causados.

d) La apropiación por el perjudicado del lucro obtenido con la intromisión ilegítima en sus derechos.

Estas medidas se entenderán sin perjuicio de la tutela cautelar necesaria para asegurar su efectividad.

Tres. La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral, que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido.

Cuatro. El importe de la indemnización por el daño moral, en el caso de los tres primeros apartados del artículo cuarto, corresponderá a las personas a que se refiere su apartado dos y, en su defecto, a sus causahabientes, en la proporción en que la sentencia estime que han sido afectados. En los casos del artículo sexto, la indemnización se entenderá comprendida en la herencia del perjudicado.

En el caso del apartado cuatro del artículo cuarto, la indemnización corresponderá a los ofendidos o perjudicados por el delito que hayan ejercitado la acción. De haberse ejercitado por el Ministerio Fiscal, éste podrá solicitar la indemnización para todos los perjudicados que hayan resultado debidamente identificados y no hayan renunciado expresamente a ella.

Cinco. Las acciones de protección frente a las intromisiones ilegítimas caducarán transcurridos cuatro años desde que el legitimado pudo ejercitarlas.

DISPOSICIÓN DEROGATORIA

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo previsto en la presente Ley Orgánica.

DISPOSICIONES TRANSITORIAS

Primera.

(Derogada)

Segunda.

En tanto no sean desarrolladas las previsiones del artículo cincuenta y tres, dos, de la Constitución sobre establecimiento de un procedimiento basado en los principios de preferencia y sumariedad, la tutela judicial de los derechos al honor, la intimidad personal y familiar y a la propia imagen se podrá recabar, con las pecualiaridades que establece esta ley sobre legitimación de las partes, por cualquiera de los procedimientos establecidos en las Secciones II y III de la Ley sesenta y dos/mil novecientos setenta y ocho, de veintiséis de diciembre, de Protección Jurisdiccional de los derechos fundamentales de la persona. Agotado el procedimiento seguido, quedará expedito el recurso de amparo constitucional en los supuestos a que se refiere el capítulo I, del Título III de la Ley Orgánica dos/mil novecientos setenta y nueve, de tres de octubre, del Tribunal Constitucional.

§ 15

Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación

Jefatura del Estado
«BOE» núm. 74, de 27 de marzo de 1984
Última modificación: sin modificaciones
Referencia: BOE-A-1984-7248

JUAN CARLOS I, REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica:

Artículo primero.

Toda persona, natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio.

Podrán ejercitar el derecho de rectificación el perjudicado aludido o su representantes y, si hubiese fallecido aquél, sus herederos o los representantes de éstos.

Artículo segundo.

El derecho se ejercitará mediante la remisión del escrito de rectificación al director del medio de comunicación dentro de los siete días naturales siguientes al de publicación o difusión de la información que se desea rectificar, de forma tal que permita tener constancias de su fecha y de su recepción.

La rectificación deberá limitarse a los hechos de la información que se desea rectificar. Su extensión no excederá sustancialmente de la de ésta, salvo que sea absolutamente necesario.

Artículo tercero.

Siempre que el derecho se ejercite de conformidad con lo establecido en el artículo anterior, el director del medio de comunicación social deberá publicar o difundir íntegramente la rectificación, dentro de los tres días siguientes al de su recepción, con relevancia semejante a aquella en que se publicó o difundió la información que se rectifica, sin comentarios ni apostillas.

Si la información que se rectifica se difundió en publicación cuya perioricidad no permita la divulgación de la rectificación en el plazo expresado, se publicará ésta en el número siguiente.

Si la noticia o información que se rectifica se difundió en espacio radiofónico o de televisión que no permita, por la periodicidad de su emisión, divulgar la rectificación en el plazo de tres días, podrá exigir el rectificante que se difunda en espacio de audiencia y relevancia semejantes, dentro de dicho plazo.

La publicación o difusión de la rectificación será siempre gratuita.

Artículo cuarto.

Si, en los plazos señalados en el artículo anterior, no se hubiera publicado o divulgado la rectificación o se hubiese notificado expresamente por el director o responsable del medio de comunicacion social que aquélla no será difundida, o se haya publicado o divulgado sin respetar lo dispuesto en el artículo anterior, podrá el perjudicado ejercitar la acción de rectificación dentro de los siete dias hábiles siguientes ante el Juez de Primera Instancia de su domicilio o ante el del lugar donde radique la dirección del medio de comunicación.

Artículo quinto.

La acción se ejercitará mediante escrito, sin necesidad de Abogado ni Procurador, acompañando la rectificación y la justificación de que se remitió en el plazo señalado; se presentará igualmente la información rectificada si se difundió por escrito; y, en otro caso, reproducción o descripción de la misma tan fiel como sea posible.

El Juez, de oficio y sin audiencia del demandado, dictará auto no admitiendo a trámite la demanda si se considera incompetente o estima la rectificación manifiestamente improcedente. En otro caso convocará al rectificante, al director del medio de comunicación o a sus representantes a juicio verbal, que se celebrará dentro de los siete días siguientes al de la petición. La convocatoria se hará telegráficamente, sin perjuicio de la urgente remisión, por cualquier otro medio, de la copia de la demanda a la parte demandada.

Cuando el Juez de Primera Instancia hubiese declarado su incompetencia podrá el perjudicado acudir al órgano competente dentro de los siete días hábiles siguientes al de la fecha de notificación de la correspondiente resolución, en la cual se deberá expresar el órgano al que corresponda el conocimiento del asunto.

Artículo sexto.

El juicio se tramitará conforme a lo establecido en la Ley de Enjuiciamiento Civil para los juicios verbales, con las siguientes modificaciones:

a) El Juez podrá reclamar de oficio que el demandado remita o presente la información enjuiciada, su grabación o reproducción escrita.

b) Sólo se admitirán las pruebas que, siendo pertinentes, puedan practicarse en el acto.

c) La sentencia se dictará en el mismo o al siguiente día del juicio.

El fallo se limitará a denegar la rectificación o a ordenar su publicación o difusión en la forma y plazos previstos en el artículo 3.º de esta Ley, contados desde la notificación de la sentencia que impondrá el pago de las costas a la parte cuyos pedimentos hubiesen sido totalmente rechazados.

La sentencia estimatoria de la petición de rectificación deberá cumplirse en sus propios términos.

El objeto de este proceso es compatible con el ejercicio de las acciones penales o civiles de otra naturaleza que pudieran asistir al perjudicado por los hechos difundidos.

Artículo séptimo.

No será necesaria la reclamación gubernativa previa cuando la información que se desea rectificar se haya publicado o difundido en un medio de comunicación de titularidad pública.

Artículo octavo.

No serán susceptibles de recurso alguno las resoluciones que dicte el Juez en este proceso, salvo el auto al que se refiere el párrafo segundo del artículo 5.º que será apelable

en ambos efectos, y la sentencia, que lo será en un solo efecto, dentro de los tres y cinco días siguientes, respectivamente, al de su notificación, conforme a lo dispuesto en las secciones primera y tercera del Título Sexto del Libro II de la Ley de Enjuiciamiento Civil. La apelación contra el auto a que se refiere el artículo 5.º se sustanciará sin audiencia del demandado.

Disposición derogatoria.

Quedan derogados los artículos 58 a 62 de la Ley 14/1966, de 18 de marzo; el artículo 25 de la Ley 4/1980, de 10 de enero, sobre el Estatuto de la Radio y la Televisión; los Decretos 745/1966, de 31 de marzo, y 746/1966, de la misma fecha, y el número 1 del artículo 566 del Código Penal, así como cuantas disposiciones se opongan a lo establecido en esta Ley.

§ 16

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. [Inclusión parcial]

Ministerio de Gracia y Justicia
«Gaceta de Madrid» núm. 206, de 25 de julio de 1889
Última modificación: 5 de junio de 2021
Referencia: BOE-A-1889-4763

Téngase en cuenta que las modificaciones realizadas al Código Civil por el artículo segundo de la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, entran en vigor el 3 de septiembre de 2021, según establece su Disposición final tercera. Ref. BOE-A-2021-9233
Téngase en cuenta que las referencias hechas a la llamada "adopción plena" se entienden sustituidas por la adopción regulada en la Ley 21/1987, de 11 de noviembre, según establece el artículo 3 de la citada Ley. Ref. BOE-A-1987-25627.

[. . .]

TÍTULO PRELIMINAR

De las normas jurídicas, su aplicación y eficacia

[. . .]

CAPÍTULO III

Eficacia general de las normas jurídicas

[. . .]

Artículo 7.

1. Los derechos deberán ejercitarse conforme a las exigencias de la buena fe.
2. La Ley no ampara el abuso del derecho o el ejercicio antisocial del mismo. Todo acto u omisión que por la intención de su autor, por su objeto o por las circunstancias en que se realice sobrepase manifiestamente los límites normales del ejercicio de un derecho, con daño para tercero, dará lugar a la correspondiente indemnización y a la adopción de las medidas judiciales o administrativas que impidan la persistencia en el abuso.

[. . .]

LIBRO CUARTO

De las obligaciones y contratos

TÍTULO I

De las obligaciones

[. . .]

CAPÍTULO II

De la naturaleza y efecto de las obligaciones

[. . .]

Artículo 1101.

Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas.

[. . .]

TÍTULO XVI

De las obligaciones que se contraen sin convenio

[. . .]

CAPÍTULO II

De las obligaciones que nacen de culpa o negligencia

Artículo 1902.

El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

[. . .]

§ 17

Ley 20/2011, de 21 de julio, del Registro Civil

Jefatura del Estado
«BOE» núm. 175, de 22 de julio de 2011
Última modificación: 3 de junio de 2021
Referencia: BOE-A-2011-12628

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La importancia del Registro Civil demanda la adopción de un nuevo modelo que se ajuste tanto a los valores consagrados en la Constitución de 1978 como a la realidad actual de la sociedad española.

Aunque la vigente Ley del Registro Civil, de 8 de junio de 1957, ha dado muestras de su calidad técnica y de su capacidad de adaptación a lo largo de estos años, es innegable que la relevancia de las transformaciones habidas en nuestro país exige un cambio normativo en profundidad que, recogiendo los aspectos más valiosos de la institución registral, la acomode plenamente a la España de hoy, cuya realidad política, social y tecnológica es completamente distinta a la de entonces.

La Constitución de 1978 sitúa a las personas y a sus derechos en el centro de la acción pública. Y ese inequívoco reconocimiento de la dignidad y la igualdad ha supuesto el progresivo abandono de construcciones jurídicas de épocas pasadas que configuraban el estado civil a partir del estado social, la religión, el sexo, la filiación o el matrimonio.

Un Registro Civil coherente con la Constitución ha de asumir que las personas –iguales en dignidad y derechos- son su única razón de ser, no sólo desde una perspectiva individual y subjetiva sino también en su dimensión objetiva, como miembros de una comunidad políticamente organizada.

Por este motivo, la Ley abandona la vieja preocupación por la constatación territorial de los hechos concernientes a las personas, sustituyéndola por un modelo radicalmente distinto que prioriza el historial de cada individuo, liberándolo de cargas administrativas y equilibrando la necesaria protección de su derecho fundamental a la intimidad con el carácter público del Registro Civil.

En este sentido, la Ley suprime el tradicional sistema de división del Registro Civil en Secciones -nacimientos, matrimonios, defunciones, tutelas y representaciones legales- y crea un registro individual para cada persona a la que desde la primera inscripción que se practique se le asigna un código personal.

Asimismo, en la presente Ley se incorpora tanto la Convención de los derechos del niño de 20 de noviembre de 1989, ratificada por España el 30 de noviembre de 1990, como la Convención sobre los derechos de las personas con discapacidad, de 13 de diciembre de 2006, ratificada por España el 23 de noviembre de 2007.

II

La modernización del Registro Civil también hace pertinente que su llevanza sea asumida por funcionarios públicos distintos de aquellos que integran el poder judicial del Estado, cuyo cometido constitucional es juzgar y ejecutar lo juzgado.

En efecto, la aplicación al Registro Civil de técnicas organizativas y de gestión de naturaleza administrativa permitirá una mayor uniformidad de criterios y una tramitación más ágil y eficiente de los distintos expedientes, sin merma alguna del derecho de los ciudadanos a una tutela judicial efectiva, pues todos los actos del Registro Civil quedan sujetos a control judicial.

Esta Ley deslinda con claridad las tradicionales funciones gubernativas y judiciales que por inercia histórica todavía aparecen entremezcladas en el sistema de la Ley de 1957, y aproxima nuestro modelo de Registro Civil al existente en otros países de nuestro entorno, en los que también se ha optado por un órgano o entidad de naturaleza administrativa con el fin de prestar un servicio público de mayor calidad, sin perjuicio de la garantía judicial de los derechos de los ciudadanos.

Puesto que la materia a la que el funcionamiento del Registro Civil se refiere es el estado civil de las personas y en ciertos aspectos, el derecho de familia, la jurisdicción competente es la civil. No obstante, se exceptúa la nacionalidad por residencia, respecto de la que persisten las razones que aconsejaron trasladar esta materia a la jurisdicción contencioso-administrativa con la entrada en vigor de la Ley 18/1990, de 17 de diciembre, de reforma del Código Civil.

III

Esa misma vocación modernizadora hace que en la Ley se diseñe un Registro Civil único para toda España, informatizado y accesible electrónicamente.

El Registro Civil se configura como una base de datos única que permite compaginar la unidad de la información con la gestión territorializada y la universalidad en el acceso. Este salto conceptual, que implica la superación del Registro físicamente articulado en libros custodiados en oficinas distribuidas por toda España, obliga a un replanteamiento de toda su estructura organizativa, que ahora ha de tener por objetivo principal eximir al ciudadano de la carga de tener que acudir presencialmente a las oficinas del Registro.

Un Registro Civil electrónico exige una estructura organizativa bien distinta de la actual. Estructura que, además, ha de tener presente a las Comunidades Autónomas.

A todo ello se dedica el título III de esta Ley, en el que se contempla una organización del Registro Civil mucho más sencilla que la anterior, diferenciándose entre Oficinas Generales, Oficina Central y Oficinas Consulares, dotadas de funciones y competencias propias, aunque dependiendo de la Dirección General de los Registros y del Notariado en tanto que centro superior directivo, consultivo y responsable último del Registro Civil.

Existirá una Oficina General por cada Comunidad o Ciudad Autónoma y otra más por cada 500.000 habitantes, al frente de la cual se encontrará un Encargado al que se le asignan las funciones de recepción de declaraciones y solicitudes, la tramitación y resolución de expedientes, la práctica de inscripciones y, en su caso, la expedición de certificaciones. A la Oficina Central le corresponde, entre otras funciones, practicar las inscripciones derivadas de resoluciones dictadas por la Dirección General de los Registros y del Notariado en los expedientes que son de su competencia. En cuanto a las Oficinas Consulares, su régimen jurídico no difiere sustancialmente del vigente.

La unidad de actuación queda garantizada mediante el carácter vinculante de las instrucciones, resoluciones y circulares de la Dirección General de los Registros y del Notariado, así como por el establecimiento de un sistema de recursos que sigue las reglas generales de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, con la previsión expresa de un recurso ante la mencionada Dirección General.

IV

La Ley concibe el Registro Civil como un registro electrónico, en el que se practican asientos informáticos, que organiza la publicidad y da fe de los hechos y actos del estado civil. Desde esta concepción se incorpora el uso de las nuevas tecnologías y de la firma electrónica.

El régimen de la publicidad del Registro Civil se articula a partir de dos instrumentos: la certificación electrónica y el acceso de la Administración, en el ejercicio de sus funciones públicas, a la información registral. Este último se concibe como el instrumento preferente de publicidad, de tal forma que sólo en casos excepcionales el ciudadano deberá presentar certificaciones de datos del Registro Civil.

El carácter electrónico del Registro Civil no significa alterar la garantía de privacidad de los datos contenidos en el mismo. Aunque el Registro Civil está excluido del ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se presta una especial protección a los datos, en tanto contengan información que afecta a la esfera de la intimidad de la persona. Lo relevante es que los datos protegidos sólo pertenecen a su titular y a él corresponde autorizar que sean facilitados a terceros.

V

En relación con los aspectos sustantivos de la Ley, merece una mención especial el título VI, relativo a hechos y actos inscribibles. Respecto de la inscripción de nacimiento, se mantienen los criterios generales y se prevé la remisión de los datos del nacido a través de un documento oficial por los responsables de los centros sanitarios. A cada nacido se le abrirá un registro individual y le será asignado un código personal.

El nombre y apellidos se configura como un elemento de identidad del nacido derivado del derecho de la personalidad y como tal se incorpora a la inscripción de nacimiento. Con el fin de avanzar en la igualdad de género se prescinde de la histórica prevalencia del apellido paterno frente al materno permitiendo que ambos progenitores sean los que decidan el orden de los apellidos. Igualmente se sistematiza y agiliza el procedimiento de cambio de nombres y apellidos y se somete, como regla general, a la competencia del Encargado del Registro Civil. En cuanto a la filiación, se elimina toda referencia a la no matrimonial, con plena equiparación a la matrimonial.

La instrucción del expediente matrimonial y la celebración del matrimonio compete a los Ayuntamientos, los cuales deberán remitir de oficio la documentación preceptiva al Registro Civil. Los Cónsules autorizarán, celebrarán e inscribirán los matrimonios de españoles en el extranjero. No se modifica la comunicación al Registro Civil de los matrimonios celebrados en forma religiosa.

De modo similar a la del nacimiento se regula la inscripción de la defunción mediante la remisión del documento oficial, acompañado de parte médico, por los centros sanitarios. Se mantiene el requisito de la práctica previa de la inscripción de fallecimiento para proceder a la inhumación o incineración.

La descentralización introducida por la Constitución de 1978 está presente, no sólo desde el punto de vista territorial, sino también desde la perspectiva de la distribución de competencias. Así, se contempla el acceso al Registro Civil de actos regulados en algunos Derechos civiles especiales como, por ejemplo, las autotutelas, apoderamientos preventivos o especialidades en materia de régimen económico del matrimonio. Igualmente, se prevé la utilización de las lenguas cooficiales, tanto en la inscripción como en la expedición de certificaciones. Además, la Ley garantiza la adecuada coexistencia de la competencia estatal

sobre Registro Civil y las de carácter ejecutivo que corresponden a las Comunidades Autónomas.

VI

La normativa de Derecho internacional privado se contiene en el título X de la Ley con una actualización de las soluciones jurídicas influidas por el avance de la legislación europea y la creciente importancia del elemento extranjero con acceso al Registro Civil. La coherencia del modelo exige a este respecto mantener la unidad, dentro de las particularidades inherentes a cada sector.

Una de las mayores novedades se centra en la inscripción de documentos judiciales extranjeros. De este modo, se permite no sólo la inscripción previo *exequátur* sino también la posibilidad de que el Encargado del Registro Civil realice la inscripción tras proceder a un reconocimiento incidental.

La complejidad inherente a las situaciones internacionales justifica que la inscripción de documentos extranjeros judiciales y no judiciales, así como de certificaciones extranjeras, corresponda con carácter exclusivo a la Oficina Central del Registro. La Oficina Central se configura además como la autoridad encargada en materia de cooperación internacional en todas aquellas materias sometidas a la Ley.

VII

El articulado se completa con disposiciones adicionales, transitorias y finales, así como con una disposición derogatoria.

Se deroga la Ley de Registro Civil de 8 de junio de 1957 que, no obstante, seguirá siendo aplicada en tanto quede extinguido el complejo régimen transitorio previsto en la Ley. De este modo se prevé un régimen de incorporación progresiva de los registros individuales y se mantienen temporalmente los efectos que el ordenamiento vigente atribuye al Libro de Familia. Igualmente se derogan expresamente los preceptos del Código civil que resultan incompatibles con las previsiones de la presente Ley.

En efecto, puesto que se prescindirá del Libro de Familia –que pierde sentido dentro del modelo moderno que se ha configurado en la presente Ley– se ha previsto que en cada registro individual conste una hoja o extracto en la que figuren los datos personales de la vida del individuo. Consecuentemente con este diseño de la hoja individual, y en la búsqueda de una mayor simplicidad y eficiencia del sistema, la Ley distingue entre las inscripciones, las anotaciones registrales y, por último, el asiento de cancelación.

Se modifica la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, a fin de determinar el órgano judicial y el procedimiento para conocer de los recursos frente a las resoluciones de la Dirección General de los Registros y del Notariado en materia de estado civil. Dichas previsiones no serán de aplicación a los recursos frente a resoluciones relativas a la adquisición de nacionalidad por residencia, cuya regulación y competencia judicial no se modifica.

La desjudicialización del Registro Civil impone la derogación del artículo 86 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial –que se lleva a cabo a través de Ley Orgánica complementaria–, y de lo previsto en la Ley 38/1998, de 28 de diciembre, de Planta y Demarcación Judicial, respecto a los Registros Civiles.

La complejidad de la Ley y el cambio radical respecto al modelo anterior aconsejan un extenso plazo de *vacatio legis,* que se ha fijado en tres años, para permitir la progresiva puesta en marcha del nuevo modelo, evitando disfunciones en el tratamiento de la información registral y la implementación de la nueva estructura organizativa.

TÍTULO I

El Registro Civil. Disposiciones generales

CAPÍTULO PRIMERO

Naturaleza, contenido y competencias del Registro Civil

Artículo 1. *Objeto de la Ley.*

La presente Ley tiene por objeto la ordenación jurídica del Registro Civil.

En particular, tiene como finalidad regular la organización, dirección y funcionamiento del Registro Civil, el acceso de los hechos y actos que se hacen constar en el mismo y la publicidad y los efectos que se otorgan a su contenido.

Artículo 2. *Naturaleza y contenido del Registro Civil.*

1. El Registro Civil es un registro público dependiente del Ministerio de Justicia. Todos los asuntos referentes al Registro Civil están encomendados a la Dirección General de los Registros y del Notariado.

Los Encargados del Registro Civil deben cumplir las órdenes, instrucciones, resoluciones y circulares del Ministerio de Justicia y de la Dirección General de los Registros y del Notariado.

2. El Registro Civil tiene por objeto hacer constar oficialmente los hechos y actos que se refieren al estado civil de las personas y aquellos otros que determine la presente Ley.

3. El contenido del Registro Civil está integrado por el conjunto de registros individuales de las personas físicas y por el resto de las inscripciones que se practiquen en el mismo conforme a lo previsto en la presente Ley.

Artículo 3. *Elementos definitorios del Registro Civil.*

1. El Registro Civil es único para toda España.

2. El Registro Civil es electrónico. Los datos serán objeto de tratamiento automatizado y se integrarán en una base de datos única cuya estructura, organización y funcionamiento es competencia del Ministerio de Justicia conforme a la presente Ley y a sus normas de desarrollo.

3. Serán de aplicación al Registro Civil las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos de carácter personal.

Artículo 4. *Hechos y actos inscribibles.*

Tienen acceso al Registro Civil los hechos y actos que se refieren a la identidad, estado civil y demás circunstancias de la persona. Son, por tanto, inscribibles:

1.º El nacimiento.
2.º La filiación.
3.º El nombre y los apellidos y sus cambios.
4.º El sexo y el cambio de sexo.
5.º La nacionalidad y la vecindad civil.
6.º La emancipación y el beneficio de la mayor edad.
7.º El matrimonio. La separación, nulidad y divorcio.
8.º El régimen económico matrimonial legal o pactado.
9.º Las relaciones paterno-filiales y sus modificaciones.
10.º Los poderes y mandatos preventivos, la propuesta de nombramiento de curador y las medidas de apoyo previstas por una persona respecto de sí misma o de sus bienes.
11.º Las resoluciones judiciales dictadas en procedimientos de provisión de medidas judiciales de apoyo a personas con discapacidad.
12.º Los actos relativos a la constitución y régimen del patrimonio protegido de las personas con discapacidad.
13.º La tutela del menor y la defensa judicial del menor emancipado.

14.º Las declaraciones de concurso de las personas físicas y la intervención o suspensión de sus facultades.

15.º Las declaraciones de ausencia y fallecimiento.

16.º La defunción.

Téngase en cuenta que esta última actualización de los puntos 10 a 16 establecida por el art. 6.1 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"10.º La modificación judicial de la capacidad de las personas, así como la que derive de la declaración de concurso de las personas físicas.

11.º La tutela, la curatela y demás representaciones legales y sus modificaciones.

12.º Los actos relativos a la constitución y régimen del patrimonio protegido de las personas con discapacidad.

13.º La autotutela y los apoderamientos preventivos.

14.º Las declaraciones de ausencia y fallecimiento.

15.º La defunción."

Artículo 5. *Registro individual.*

1. Cada persona tendrá un registro individual en el que constarán los hechos y actos relativos a la identidad, estado civil y demás circunstancias en los términos de la presente Ley.

2. El registro individual se abrirá con la inscripción de nacimiento o con el primer asiento que se practique.

3. En dicho registro se inscribirán o anotarán, continuada, sucesiva y cronológicamente, todos los hechos y actos que tengan acceso al Registro Civil.

Artículo 6. *Código personal.*

A cada registro individual abierto con el primer asiento que se practique se le asignará un código personal constituido por la secuencia alfanumérica generada por el Registro Civil, que será única e invariable en el tiempo.

Artículo 7. *Firma electrónica.*

1. Los Encargados del Registro Civil dispondrán de certificados electrónicos cualificados. Mediante dichos certificados electrónicos se firmarán los asientos del Registro Civil con firma electrónica avanzada. Las certificaciones de las inscripciones electrónicas, o las que se expidan por medios electrónicos, serán selladas directamente por el sistema, con sello electrónico avanzado basado en un certificado de sello electrónico cualificado, salvo en los supuestos en que esta opción no sea posible, en cuyo caso serán firmadas por el Encargado con firma electrónica avanzada mediante su certificado electrónico cualificado.

Así mismo, el personal del Registro Civil que se determine reglamentariamente podrá disponer de certificado electrónico cualificado con firma electrónica avanzada.

2. Se garantizará la verificabilidad de las firmas y sellos electrónicos de dichos asientos, incluso una vez haya caducado o se haya revocado el certificado con el cual se practicó el asiento, mediante la utilización de formatos o servicios que preserven la longevidad de firmas y sellos electrónicos durante el tiempo exigido por la legislación vigente.

3. Las personas podrán identificarse electrónicamente ante el Registro Civil a través de cualquiera de los sistemas previstos en el artículo 9 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como en la normativa vigente en materia de identificación y firma electrónica.

Artículo 8. *Comunicación entre las Oficinas del Registro Civil y con las Administraciones Públicas.*

1. Las Oficinas del Registro Civil se comunicarán entre sí a través de medios electrónicos.
2. Todas las Administraciones y funcionarios públicos, en el ejercicio de sus competencias y bajo su responsabilidad, tendrán acceso a los datos que consten en el Registro Civil único con las excepciones relativas a los datos especialmente protegidos previstas en esta Ley. Dicho acceso se efectuará igualmente mediante procedimientos electrónicos con los requisitos y prescripciones técnicas que sean establecidas dentro del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad.

Artículo 9. *Competencias generales del Registro Civil.*

En el Registro Civil constarán los hechos y actos inscribibles que afectan a los españoles y los referidos a extranjeros, acaecidos en territorio español.
Igualmente, se inscribirán los hechos y actos que hayan tenido lugar fuera de España, cuando las correspondientes inscripciones sean exigidas por el Derecho español.

Artículo 10. *Reglas de competencia.*

1. La solicitud de inscripción y la práctica de la misma se podrán efectuar en cualquiera de las Oficinas Generales del Registro Civil con independencia del lugar en el que se produzcan los hechos o actos inscribibles. Si se producen en el extranjero, la inscripción se solicitará y, en su caso, se practicará en la Oficina Consular de la circunscripción correspondiente. En este último caso, la inscripción también se podrá solicitar y practicar en cualquiera de las Oficinas Generales.
2. Los ciudadanos podrán solicitar en cualquiera de las Oficinas del Registro Civil o por medios electrónicos el acceso a la información contenida en el mismo a través de los medios de publicidad previstos en esta Ley.

CAPÍTULO SEGUNDO

Derechos y deberes ante el Registro Civil

Artículo 11. *Derechos ante el Registro Civil.*

Son derechos de las personas ante el Registro Civil:

a) El derecho a un nombre y a ser inscrito mediante la apertura de un registro individual y la asignación de un código personal.
b) El derecho a la inscripción de los hechos y actos que se refieren a su identidad, estado civil y demás circunstancias personales que la Ley prevea.
c) El derecho a acceder a la información que solicite sobre el contenido del Registro, con las limitaciones previstas en la presente Ley.
d) El derecho a obtener certificaciones.
e) El derecho a la intimidad en relación con datos especialmente protegidos sometidos a régimen de publicidad restringida.
f) El derecho a acceder a los servicios del Registro Civil en cualquiera de las Oficinas Generales o Consulares del Registro Civil.
g) El derecho a utilizar ante el Registro Civil cualquiera de las lenguas oficiales en el lugar donde radique la Oficina.
h) El derecho a la igualdad de género y al pleno reconocimiento del principio de igualdad, en todas sus manifestaciones, en materia de Derecho del Registro Civil.
i) El derecho a promover la inscripción de determinados hechos y actos dirigidos a la protección de los menores, las personas mayores y otras personas respecto de las cuales la inscripción registral supone una particular garantía de sus derechos.

Téngase en cuenta que esta última actualización de la letra i) establecida por el art. 6.2 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:
"i) El derecho a promover la inscripción de determinados hechos y actos dirigidos a la protección de los menores, personas con capacidad modificada judicialmente, personas con discapacidad y personas mayores."

j) El derecho a promover la rectificación o modificación de los asientos registrales en los casos legal o reglamentariamente previstos.
k) El derecho a interponer recursos en los términos previstos en la presente Ley.
l) El derecho a acceder a los servicios del Registro Civil con garantía de los principios de accesibilidad universal y diseño para todas las personas.

Artículo 12. *Deberes ante el Registro Civil.*

Son deberes de las personas ante el Registro Civil:

a) El deber de promover la práctica de los asientos registrales en los casos previstos en la presente Ley.
b) El deber de instar la inscripción cuando ésta tenga carácter constitutivo en los casos legalmente previstos.
c) El deber de comunicar los hechos y actos inscribibles conforme a lo previsto en la presente Ley.
d) El deber de presentar la documentación necesaria cuando los datos correspondientes no obren en poder de las Administraciones Públicas.
e) El deber de suministrar datos veraces y exactos en las solicitudes de inscripción o en cumplimiento de los deberes a los que se refieren los números anteriores.
f) El deber de cooperar en el buen funcionamiento del Registro Civil como servicio público.

TÍTULO II

Principios de funcionamiento del Registro Civil

Artículo 13. *Principio de legalidad.*

Los Encargados del Registro Civil comprobarán de oficio la realidad y legalidad de los hechos y actos cuya inscripción se pretende, según resulte de los documentos que los acrediten y certifiquen, examinando en todo caso la legalidad y exactitud de dichos documentos.

Artículo 14. *Principio de oficialidad.*

Los Encargados del Registro Civil deberán practicar la inscripción oportuna cuando tengan en su poder los títulos necesarios.
Las personas físicas y jurídicas y los organismos e instituciones públicas que estén obligados a promover las inscripciones facilitarán a los Encargados del Registro Civil los datos e información necesarios para la práctica de aquéllas.

Artículo 15. *Principio de publicidad.*

1. Los ciudadanos tendrán libre acceso a los datos que figuren en su registro individual.
2. El Registro Civil es público. Las Administraciones y funcionarios públicos, para el desempeño de sus funciones y bajo su responsabilidad, podrán acceder a los datos contenidos en el Registro Civil.

3. También podrá obtenerse información registral, por los medios de publicidad previstos en los artículos 80 y siguientes de la presente Ley, cuando se refieran a persona distinta del solicitante, siempre que conste la identidad del solicitante y exista un interés legítimo.

4. Quedan exceptuados del régimen general de publicidad los datos especialmente protegidos, que estarán sometidos al sistema de acceso restringido al que se refieren los artículos 83 y 84 de la presente Ley.

Artículo 16. *Presunción de exactitud.*

1. Los Encargados del Registro Civil están obligados a velar por la concordancia entre los datos inscritos y la realidad extraregistral.

2. Se presume que los hechos inscritos existen y los actos son válidos y exactos mientras el asiento correspondiente no sea rectificado o cancelado en la forma prevista por la ley.

3. Cuando se impugnen judicialmente los actos y hechos inscritos en el Registro Civil, deberá instarse la rectificación del asiento correspondiente.

Artículo 17. *Eficacia probatoria de la inscripción.*

1. La inscripción en el Registro Civil constituye prueba plena de los hechos inscritos.

2. Sólo en los casos de falta de inscripción o en los que no fuera posible certificar del asiento, se admitirán otros medios de prueba.

En el primer caso, será requisito indispensable para su admisión la acreditación de que previa o simultáneamente se ha instado la inscripción omitida o la reconstrucción del asiento, y no su mera solicitud.

Artículo 18. *Eficacia constitutiva de la inscripción en el Registro Civil.*

La inscripción en el Registro Civil sólo tendrá eficacia constitutiva en los casos previstos por la Ley.

Artículo 19. *Presunción de integridad. Principio de inoponibilidad.*

1. El contenido del Registro Civil se presume íntegro respecto de los hechos y actos inscritos.

2. En los casos legalmente previstos, los hechos y actos inscribibles conforme a las prescripciones de esta Ley serán oponibles a terceros desde que accedan al Registro Civil.

TÍTULO III

Estructura y dependencia del Registro Civil

CAPÍTULO PRIMERO

Oficinas del Registro Civil

Artículo 20. *Estructura del Registro Civil.*

1. El Registro Civil depende del Ministerio de Justicia y se organiza en:

1.º Oficina Central.
2.º Oficinas Generales.
3.º Oficinas Consulares.

2. Las inscripciones y demás asientos registrales serán practicados por los Encargados de las Oficinas del Registro Civil.

Bajo su responsabilidad y en los términos y con los límites que reglamentariamente se determinen, el Encargado podrá delegar funciones en el personal al servicio de la Oficina del Registro Civil.

3. Los ciudadanos podrán presentar la solicitud y la documentación requerida ante cualquier Oficina del Registro Civil o remitirla electrónicamente. Igualmente, podrán

presentar en las Oficinas Colaboradoras la solicitud y la documentación necesaria para las actuaciones ante el Registro Civil.

Artículo 21. *Oficina Central del Registro Civil.*

1. El Ministerio de Justicia designará a los Encargados de la Oficina Central del Registro Civil.
2. La Oficina Central del Registro Civil desempeña las siguientes funciones:

1.ª Practicar las inscripciones que se deriven de resoluciones dictadas por la Dirección General de los Registros y del Notariado, referidas a hechos o actos susceptibles de inscripción en el Registro Civil.
2.ª Practicar la inscripción de los documentos auténticos extranjeros judiciales y extrajudiciales y certificaciones de asientos extendidos en Registros extranjeros, salvo aquellos cuya competencia pueda corresponder a las Oficinas Consulares del Registro Civil.
3.ª Practicar la inscripción de fallecimiento de las personas de nacionalidad extranjera al servicio de las Fuerzas Armadas y de las Fuerzas y Cuerpos de Seguridad, siempre que dicho fallecimiento hubiera ocurrido durante una misión u operación fuera de España y que el sistema registral del Estado donde se produjo el hecho no practicare la pertinente inscripción. Lo anterior será sin perjuicio de trasladar la inscripción realizada al Registro del Estado del cual fuere nacional la persona fallecida.
4.ª También desempeñará todas aquellas funciones que le sean atribuidas por las leyes.

3. La Oficina Central es la autoridad encargada en materia de cooperación internacional sobre Registro Civil en los términos previstos por los instrumentos internacionales aplicables en España y la presente Ley.

Artículo 22. *Oficinas Generales del Registro Civil.*

1. Existirá una Oficina General del Registro Civil en todas las poblaciones que sean sede de la capital de un partido judicial.
2. Al frente de cada Oficina General del Registro Civil estará un Encargado del Registro Civil, que ejercerá sus cometidos bajo la dependencia funcional de la Dirección General de Seguridad Jurídica y Fe Pública. Por necesidades del servicio se podrá designar más de un Encargado en una Oficina, en cuyo caso se incluirá en la correspondiente relación de puestos de trabajo la consideración de uno de los puestos de encargado como Encargado coordinador sin relevación de funciones, a efectos de organización interna y distribución de tareas conforme a las instrucciones o protocolos que apruebe la Dirección General de Seguridad Jurídica y Fe Pública.
3. Son funciones de las Oficinas Generales del Registro Civil:

a) Recibir y documentar declaraciones de conocimiento y de voluntad en materias propias de su competencia, así como expedir certificaciones.
b) Recibir por vía electrónica o presencial solicitudes o formularios, así como otros documentos que sirvan de título para practicar un asiento en el Registro Civil.
c) Tramitar y resolver los expedientes de Registro Civil que les atribuya el ordenamiento jurídico.
d) Practicar las inscripciones y demás asientos de su competencia.
e) Expedir certificaciones de los asientos registrales.
f) Cualesquiera otras funciones que les atribuya la Dirección General de Seguridad Jurídica y Fe Pública.

Artículo 23. *Oficinas Consulares del Registro Civil.*

Las Oficinas Consulares del Registro Civil estarán a cargo de los Cónsules de España o, en su caso, de los funcionarios diplomáticos encargados de las Secciones consulares de la Misión Diplomática.

Artículo 24. *Funciones de las Oficinas Consulares del Registro Civil.*

Son funciones de los Registros Consulares:

1.ª Inscribir los hechos y actos relativos a españoles acaecidos en su circunscripción consular, así como los documentos extranjeros judiciales y no judiciales y certificaciones de Registros Civiles extranjeros que sirvan de título para practicar la inscripción.

2.ª Expedir certificaciones de los asientos registrales.

3.ª Recibir y documentar declaraciones de conocimiento y de voluntad en materias propias de su competencia.

4.ª Instruir el expediente previo de matrimonio, así como expedir los certificados de capacidad necesarios para su celebración en el extranjero.

5.ª Comunicar a la Dirección General de los Registros y del Notariado la legislación extranjera vigente en materia vinculada al estado civil de las personas.

CAPÍTULO SEGUNDO

La Dirección General de los Registros y del Notariado

Artículo 25. *La Dirección General de los Registros y del Notariado.*

La Dirección General de los Registros y del Notariado es el centro directivo y consultivo del Registro Civil de España.

Artículo 26. *Funciones de la Dirección General de los Registros y del Notariado en el Registro Civil.*

En materia de Registro Civil, son funciones de la Dirección General de los Registros y del Notariado las siguientes:

1.ª Promover la elaboración de disposiciones de carácter general.

2.ª Dictar las instrucciones, resoluciones y circulares que estime procedentes en los asuntos de su competencia, que tendrán carácter vinculante.

3.ª Supervisar y coordinar el cumplimiento de las normas registrales por el Encargado y demás personal al servicio de las Oficinas del Registro Civil.

4.ª Resolver los recursos legalmente previstos y atender las consultas que se planteen acerca de la interpretación y ejecución de la legislación en materia de Registro Civil.

5.ª Resolver los expedientes de su competencia en materia de Registro Civil.

6.ª Ordenar la planificación estratégica, y coordinar las actuaciones en esta materia con otras Administraciones e instituciones públicas o privadas.

7.ª Implantar y elaborar programas de calidad del servicio público que presta el Registro Civil.

8.ª Cualesquiera otras que le atribuyan las leyes.

TÍTULO IV

Títulos que acceden al Registro Civil. Control de legalidad

CAPÍTULO PRIMERO

Títulos que acceden al Registro Civil

Artículo 27. *Documentos auténticos para practicar inscripciones.*

1. El documento auténtico, sea original o testimonio, sea judicial, administrativo, notarial o registral, es título suficiente para inscribir el hecho o acto que accede al Registro Civil.

También es título suficiente para practicar la inscripción el documento extranjero que cumpla los requisitos establecidos en los artículos 96 y 97 de la presente Ley.

2. Las resoluciones judiciales firmes son títulos suficientes para inscribir el hecho o acto que constituyen o declaran. Si contradicen hechos inscritos, debe practicarse la rectificación correspondiente.

3. Los documentos a los que se refieren los dos apartados anteriores podrán presentarse en cualquier soporte, incluido el electrónico, siempre que cumplan los requisitos, formato y eficacia previstos en sus respectivas normas reguladoras.

4. Los documentos presentados en las Oficinas del Registro Civil y en las Oficinas Colaboradoras se custodiarán y conservarán en los términos establecidos por la normativa reguladora de esta materia para las Administraciones Públicas.

Artículo 28. *Certificaciones de Registros extranjeros.*

Para practicar inscripciones sin expediente, en virtud de certificación de Registro extranjero, será necesario el cumplimiento de los requisitos establecidos en la normativa aplicable para que tenga eficacia en España.

Artículo 29. *Declaraciones de las personas obligadas.*

1. Las declaraciones en virtud de las cuales hayan de practicarse los asientos se consignarán en acta firmada por el funcionario competente de la Oficina General o Consular y por los declarantes, o bien mediante la cumplimentación del formulario oficialmente aprobado.
2. La verificación de las declaraciones comprenderá la capacidad e identidad del declarante.

CAPÍTULO SEGUNDO

Control de legalidad

Artículo 30. *Control de legalidad de los documentos.*

1. Los obligados a promover la inscripción sólo tendrán que aportar los documentos exigidos por la ley cuando los datos incorporados a los mismos no constaren en el Registro Civil o no pudieran ser facilitados por otras Administraciones o funcionarios públicos.
2. El Encargado de la Oficina del Registro Civil ante el que se solicita la inscripción deberá controlar la legalidad de las formas extrínsecas del documento, la validez de los actos y la realidad de los hechos contenidos en éste.
La calificación de las sentencias y resoluciones judiciales recaerá sobre la competencia y clase del procedimiento seguido, formalidades extrínsecas de los documentos presentados y asientos del propio Registro.
3. Si el Encargado de la Oficina del Registro Civil tuviere fundadas dudas sobre la legalidad de los documentos, sobre la veracidad de los hechos o sobre la exactitud de las declaraciones, realizará antes de extender la inscripción, y en el plazo de diez días, las comprobaciones oportunas.
Si de la verificación de los documentos y declaraciones efectuadas se dedujera una contradicción esencial entre el Registro y la realidad, el Encargado del Registro Civil lo pondrá en conocimiento del Ministerio Fiscal y lo advertirá a los interesados.

Artículo 31. *Examen de las solicitudes de inscripción y de las declaraciones.*

En el examen de las solicitudes y de las declaraciones que se formulen, la Oficina Consular o General del Registro Civil verificará la identidad y capacidad de los solicitantes o declarantes y, en su caso, comprobará la autenticidad de la firma.

Artículo 32. *Constancia de solicitudes y declaraciones efectuadas en las Oficinas del Registro Civil.*

1. Las solicitudes y declaraciones que formulen los ciudadanos a través de cualquiera de los medios previstos en esta Ley ante las Oficinas del Registro Civil quedarán debidamente registradas en la forma que reglamentariamente se determine.
En todo caso, deberá quedar constancia de la identidad y domicilio del solicitante o declarante, del Documento nacional de identidad o Número de identificación del extranjero, de la fecha en la que se ha formulado la solicitud o declaración, del contenido de ésta y de la actuación del funcionario de la oficina a la que se haya dirigido.
2. A esta información deberán acceder todas las Oficinas del Registro Civil, que denegarán al interesado la inscripción solicitada o la recepción de la declaración sobre la

que el funcionario o funcionarios competentes de una oficina ya se hubiera pronunciado o hubiese sido requerida para hacerlo.

TÍTULO V

Los asientos registrales

CAPÍTULO PRIMERO

Competencia para efectuar los asientos

Artículo 33. *Regla general para la práctica de los asientos.*

1. El Encargado de la Oficina del Registro Civil ante el que se presente el título o se formule la declaración practicará los asientos correspondientes de oficio o dictará resolución denegándolos en el plazo de cinco días. La inscripción de la defunción, no existiendo obstáculo legal, se practicará en el mismo día de la presentación de la documentación. En las Oficinas Consulares del Registro Civil, para las inscripciones referentes a nacionalidad y matrimonio, los asientos se practicarán en el plazo más breve posible.

2. Sin perjuicio de lo dispuesto en el apartado anterior, el Encargado de la Oficina Central practicará los asientos a los que den lugar las resoluciones dictadas en los expedientes para cuya tramitación y resolución sea competente el Ministerio de Justicia.

Artículo 34. *Asientos de resoluciones judiciales.*

El letrado de la Administración de Justicia del órgano judicial que haya dictado una resolución cuyo contenido deba causar asiento en el Registro Civil por afectar al estado civil de las personas, deberá remitir por medios electrónicos a la Oficina del Registro Civil testimonio o copia electrónica de la resolución judicial referida.

Artículo 35. *Inscripción de documentos notariales.*

Los Notarios, dentro de su ámbito de competencias, remitirán por medios electrónicos a la Oficina General del Registro Civil los documentos públicos que den lugar a asiento en el Registro Civil.

CAPÍTULO SEGUNDO

Reglas generales para la práctica de asientos

Artículo 36. *Asientos electrónicos.*

1. En el Registro Civil todos los asientos se extenderán en soporte y formato electrónico. Dichos asientos deberán ajustarse a los modelos aprobados por la Dirección General de los Registros y del Notariado.

2. En circunstancias excepcionales y cuando no sea posible practicar asientos electrónicos, el asiento podrá efectuarse en soporte papel. En este caso, se trasladará al formato electrónico con la mayor celeridad posible.

3. Los asientos en el Registro Civil deben archivarse después de su cierre en un registro electrónico de seguridad.

Artículo 37. *Lenguas oficiales.*

Los ciudadanos que insten la inscripción de un hecho o acto en el Registro Civil, podrán solicitar que la misma se practique en cualquiera de las lenguas oficiales del lugar donde radique la Oficina General del Registro Civil.

CAPÍTULO TERCERO

Clases de asientos

Artículo 38. *Clases de asientos.*

Los asientos del Registro Civil son las inscripciones, las anotaciones y las cancelaciones.

Artículo 39. *Inscripciones.*

1. La inscripción es la modalidad de asiento a través de la cual acceden al Registro Civil los hechos y actos relativos al estado civil de las personas y aquellos otros determinados por esta Ley.
2. Los efectos de la inscripción son los previstos en los artículos 17 y 18 de la presente Ley.

Artículo 40. *Anotaciones registrales.*

1. Las anotaciones registrales son la modalidad de asiento que en ningún caso tendrá el valor probatorio que proporciona la inscripción. Tendrán un valor meramente informativo, salvo los casos en que la Ley les atribuya valor de presunción.
2. Las anotaciones registrales se extenderán a petición del Ministerio Fiscal o de cualquier interesado.
3. Pueden ser objeto de anotación los siguientes hechos y actos:

1.º El procedimiento judicial, administrativo o registral en trámite que pueda afectar al contenido del Registro Civil.
2.º El hecho cuya inscripción no pueda extenderse por no resultar, en alguno de sus extremos, legalmente acreditado.
3.º Las declaraciones con valor de presunción.
4.º El hecho o acto relativo a españoles o acaecido en España que afecte a su estado civil, según la ley extranjera.
5.º La sentencia o resolución extranjera que afecte al estado civil, en tanto no se obtenga el *exequátur* o el reconocimiento incidental en España.
6.º La sentencia o resolución canónica cuya ejecución en cuanto a efectos civiles no haya sido decretada aún por el Tribunal correspondiente.
7.º La desaparición.
8.º Las actuaciones tutelares y de otras figuras tuitivas previstas en la Ley, en los casos que reglamentariamente se determinen.
9.º El acogimiento, la guarda administrativa y la guarda de hecho.
10.º Aquellos otros hechos o actos cuya anotación se prevea en esta u otra ley.

Artículo 41. *Cancelaciones.*

Los asientos de cancelación privan de eficacia, total o parcial, al asiento registral de cualquier clase por nulidad del propio asiento, por ineficacia o inexistencia del hecho o del acto o por cualquier otra causa establecida por la ley.

La cancelación se practicará en virtud de título adecuado, ya sea de oficio o a solicitud del interesado.

CAPÍTULO CUARTO

Promoción de la inscripción y de otros asientos

Artículo 42. *Personas obligadas a promover la inscripción.*

1. Están obligados a promover sin demora la inscripción:

1.º Los designados en cada caso por la ley.
2.º Aquellos a quienes se refiere el hecho inscribible, sus herederos o representantes legales.

3.º El Ministerio Fiscal en el ejercicio de sus funciones con arreglo a las previsiones de esta Ley.

2. Las autoridades y funcionarios no comprendidos en el número anterior, a quienes consten por razón de sus cargos los hechos no inscritos, están obligados a comunicarlos al Ministerio Fiscal.

Artículo 43. *Comunicación de hechos y actos al Registro Civil.*

Las personas obligadas a promover la inscripción deberán comunicar los hechos y actos inscribibles, bien mediante la presentación de los formularios oficiales debidamente cumplimentados, bien mediante su remisión por medios electrónicos en la forma que reglamentariamente se determine, acompañando los documentos acreditativos que en cada caso se establezca.

También procederá la inscripción a instancia de cualquier persona que presente título suficiente.

TÍTULO VI

Hechos y actos inscribibles

CAPÍTULO PRIMERO

Inscripción de nacimiento

Sección 1.ª Hecho inscribible y personas obligadas a promover la inscripción

Artículo 44. *Inscripción de nacimiento y filiación.*

1. Son inscribibles los nacimientos de las personas, conforme a lo previsto en el artículo 30 del Código Civil.

2. La inscripción hace fe del hecho, fecha, hora y lugar del nacimiento, identidad, sexo y, en su caso, filiación del inscrito.

3. La inscripción de nacimiento se practicará en virtud de declaración formulada en documento oficial debidamente firmado por el o los declarantes, acompañada del parte facultativo. A tal fin, el médico, el enfermero especialista en enfermería obstétrico-ginecológica o el enfermero que asista al nacimiento, dentro o fuera del establecimiento sanitario, comprobará, por cualquiera de los medios admitidos en derecho, la identidad de la madre del recién nacido a los efectos de su inclusión en el parte facultativo. Los progenitores realizarán su declaración mediante la cumplimentación del correspondiente formulario oficial, en el que se contendrán las oportunas advertencias sobre el valor de tal declaración conforme a las normas sobre determinación legal de la filiación.

En defecto del parte facultativo, deberá aportarse la documentación acreditativa en los términos que reglamentariamente se determinen.

El Encargado del Registro Civil, una vez recibida y examinada la documentación, practicará inmediatamente la inscripción de nacimiento. Tal inscripción determinará la apertura de un nuevo registro individual, al que se asignará un código personal en los términos previstos en el artículo 6 de la presente Ley.

4. La filiación se determinará, a los efectos de la inscripción de nacimiento, de conformidad con lo establecido en las leyes civiles y en la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida.

Salvo en los casos a que se refiere el artículo 48, en toda inscripción de nacimiento ocurrida en España se hará constar necesariamente la filiación materna, aunque el acceso a la misma será restringido en los supuestos en que la madre por motivos fundados así lo solicite y siempre que renuncie a ejercer los derechos derivados de dicha filiación. En caso de discordancia entre la declaración y el parte facultativo o comprobación reglamentaria, prevalecerá este último.

La filiación paterna en el momento de la inscripción del hijo, se hará constar:

a) Cuando conste debidamente acreditado el matrimonio con la madre y resulte conforme con las presunciones de paternidad del marido establecidas en la legislación civil o, aun faltando aquellas, en caso de que concurra el consentimiento de ambos cónyuges, aunque existiera separación legal o de hecho.

b) Cuando el padre manifieste su conformidad a la determinación de tal filiación, siempre que la misma no resulte contraria a las presunciones establecidas en la legislación civil y no existiere controversia. Deberán cumplirse, además, las condiciones previstas en la legislación civil para su validez y eficacia.

En los supuestos en los que se constate que la madre tiene vínculo matrimonial con persona distinta de la que figura en la declaración o sea de aplicación la presunción prevista en el artículo 116 del Código civil se practicará la inscripción de nacimiento de forma inmediata sólo con la filiación materna y se procederá a la apertura de un expediente registral para la determinación de la filiación paterna.

5. También constará como filiación matrimonial cuando la madre estuviere casada, y no separada legalmente o de hecho, con otra mujer y esta última manifestara que consiente en que se determine a su favor la filiación respecto al hijo nacido de su cónyuge.

6. En los casos de filiación adoptiva se hará constar, conforme a la legislación aplicable, la resolución judicial o administrativa que constituya la adopción, quedando sometida al régimen de publicidad restringida previsto en la presente Ley.

7. El reconocimiento de la filiación no matrimonial con posterioridad a la inscripción de nacimiento podrá hacerse en cualquier tiempo con arreglo a las formas establecidas en la legislación civil aplicable. Si se realizare mediante declaración del padre ante el encargado del Registro Civil, se requerirá el consentimiento expreso de la madre y del representante legal si fuera menor de edad o de la persona a la que se reconoce si fuera mayor. Si se tratare de personas con discapacidad respecto de las cuales se hubiesen establecido medidas de apoyo, se estará a lo que resulte de la resolución judicial que las haya establecido o del documento notarial en el que se hayan previsto o acordado. Para que sea posible la inscripción deberán concurrir, además, los requisitos para la validez o eficacia del reconocimiento exigidos por la legislación civil.

Téngase en cuenta que esta última actualización del primer párrafo del apartado 7 establecida por el art. 6.3 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"7. El reconocimiento de la filiación no matrimonial con posterioridad a la inscripción del hijo podrá hacerse con arreglo a las formas establecidas en el Código Civil en cualquier tiempo. Si se realizare mediante declaración del padre ante el Encargado del Registro Civil, se requerirá el consentimiento expreso de la madre y del representante legal del hijo si fuera menor de edad o de este si fuera mayor. Si tuviera la capacidad modificada judicialmente se precisará, según la sentencia, el consentimiento de su representante legal, el asentimiento de su curador o el consentimiento del hijo. Para que sea posible la inscripción deberán concurrir, además, los requisitos para la validez o eficacia del reconocimiento exigidos por la Ley civil."

Podrá inscribirse la filiación mediante expediente aprobado por el Encargado del Registro Civil, siempre que no haya oposición del Ministerio Fiscal o de parte interesada notificada personal y obligatoriamente, si concurre alguna de las siguientes circunstancias:

1.ª Cuando exista escrito indubitado del padre o de la madre en que expresamente reconozca la filiación.

2.ª Cuando el hijo se halle en la posesión continua del estado de hijo del padre o de la madre, justificada por actos directos del mismo padre o de su familia.

3.ª Respecto de la madre, siempre que se pruebe cumplidamente el hecho del parto y la identidad del hijo.

Formulada oposición, la inscripción de la filiación sólo podrá obtenerse por el procedimiento regulado en la Ley de Enjuiciamiento Civil.

8. En los supuestos de controversia y en aquellos otros que la ley determine, para hacer constar la filiación paterna se requerirá previa resolución judicial dictada conforme a las disposiciones previstas en la legislación procesal.

9. Una vez practicada la inscripción, el Encargado expedirá certificación literal electrónica de la inscripción de nacimiento y la pondrá a disposición del declarante o declarantes.

Artículo 45. *Obligados a promover la inscripción de nacimiento.*

Están obligados a promover la inscripción de nacimiento:

1. La dirección de hospitales, clínicas y establecimientos sanitarios.

2. El personal médico o sanitario que haya atendido el parto, cuando éste haya tenido lugar fuera de establecimiento sanitario.

3. Los progenitores. No obstante, en caso de renuncia al hijo en el momento del parto, la madre no tendrá esta obligación, que será asumida por la Entidad Pública correspondiente.

4. El pariente más próximo o, en su defecto, cualquier persona mayor de edad presente en el lugar del alumbramiento al tiempo de producirse.

Artículo 46. *Comunicación del nacimiento por los centros sanitarios.*

La dirección de hospitales, clínicas y establecimientos sanitarios comunicará en el plazo de setenta y dos horas a la Oficina del Registro Civil que corresponda cada uno de los nacimientos que hayan tenido lugar en el centro sanitario, excepto aquellos casos que exijan personarse ante el Encargado del Registro Civil. El personal sanitario que asista al nacimiento deberá adoptar, bajo su responsabilidad, las cautelas necesarias para asegurar la identificación del recién nacido y efectuará las comprobaciones que establezcan de forma indubitada la relación de filiación materna, incluyendo, en su caso, las pruebas biométricas, médicas y analíticas que resulten necesarias para ello conforme a la legislación reguladora de las historias clínicas. En todo caso se tomarán las dos huellas plantares del recién nacido junto a las huellas dactilares de la madre para que figuren en el mismo documento. En la inscripción que del nacimiento se practique en el Registro Civil se hará constar la realización de dichas pruebas y el centro sanitario que inicialmente conserve la información relacionada con las mismas, sin perjuicio del traslado de esta información a los archivos definitivos de la administración correspondiente cuando proceda.

Cumplidos los requisitos, la comunicación se realizará mediante la remisión electrónica del formulario oficial de declaración debidamente cumplimentado por el centro sanitario y firmado por la persona o personas que tengan la obligación de comunicar el nacimiento, que comprenderá la identificación y nacionalidad de los declarantes, y sus declaraciones relativas al nombre elegido para el recién nacido, el orden de sus apellidos y su filiación paterna. A este formulario se incorporará el parte acreditativo del nacimiento firmado por el facultativo que hubiese asistido al parto. Dicha remisión será realizada por personal del centro sanitario, que usará para ello mecanismos seguros de identificación y firma electrónicos.

Simultáneamente a la presentación de los citados formularios oficiales, se remitirán al Instituto Nacional de Estadística los datos requeridos a efectos de las competencias asignadas por la Ley a dicho Instituto.

Los firmantes estarán obligados a acreditar su identidad ante el personal sanitario que hubiere asistido al nacimiento, bajo la responsabilidad del mismo, por los medios admitidos en Derecho.

Artículo 47. *Inscripción de nacimiento por declaración de otras personas obligadas.*

1. Respecto de los nacimientos que se hayan producido fuera de establecimiento sanitario, o cuando por cualquier causa no se haya remitido el documento en el plazo y condiciones previstos en el artículo anterior, los obligados a promover la inscripción dispondrán de un plazo de diez días para declarar el nacimiento ante la Oficina del Registro Civil o las Oficinas Consulares de Registro Civil.

2. La declaración se efectuará presentando el documento oficial debidamente cumplimentado acompañado del certificado médico preceptivo firmado electrónicamente por el facultativo o, en su defecto, del documento acreditativo en los términos que reglamentariamente se determinen.

3. Para inscribir la declaración, cuando haya transcurrido desde el nacimiento el plazo previsto, se precisará resolución dictada en expediente registral.

Artículo 48. *Menores abandonados y menores no inscritos.*

1. Las entidades públicas de las Comunidades Autónomas competentes en materia de protección de menores deberán promover sin demora la inscripción de menores en situación de desamparo por abandono, sea o no conocida su filiación, así como la inscripción de la tutela administrativa que, en su caso, asuman, sin perjuicio de la anotación de la guarda que deban asumir.

2. El Ministerio Fiscal promoverá igualmente la inscripción de menores no inscritos.

Sección 2.ª Contenido de la inscripción de nacimiento

Artículo 49. *Contenido de la inscripción de nacimiento y atribución de apellidos.*

1. En la inscripción de nacimiento constarán los datos de identidad del nacido consistentes en el nombre que se le impone y los apellidos que le correspondan según su filiación. Constarán asimismo el lugar, fecha y hora del nacimiento y el sexo del nacido.

2. La filiación determina los apellidos.

Si la filiación está determinada por ambas líneas, los progenitores acordarán el orden de transmisión de su respectivo primer apellido, antes de la inscripción registral.

En caso de desacuerdo o cuando no se hayan hecho constar los apellidos en la solicitud de inscripción, el Encargado del Registro Civil requerirá a los progenitores, o a quienes ostenten la representación legal del menor, para que en el plazo máximo de tres días comuniquen el orden de apellidos. Transcurrido dicho plazo sin comunicación expresa, el Encargado acordará el orden de los apellidos atendiendo al interés superior del menor.

En los supuestos de nacimiento con una sola filiación reconocida, ésta determina los apellidos. El progenitor podrá determinar el orden de los apellidos.

El orden de los apellidos establecido para la primera inscripción de nacimiento determina el orden para la inscripción de los posteriores nacimientos con idéntica filiación. En esta primera inscripción, cuando así se solicite, podrán constar la preposición «de» y las conjunciones «y» o «i»entre los apellidos, en los términos previstos en el artículo 53 de la presente Ley.

3. También se incorporará a la inscripción el código personal asignado.

4. Constarán, además, y siempre que fuera posible, las siguientes circunstancias de los progenitores: nombre y apellidos, Documento Nacional de Identidad o Número de identificación y pasaporte del extranjero, en su caso, lugar y fecha de nacimiento, estado civil, domicilio y nacionalidad, así como cualquier otro dato necesario para el cumplimiento del objeto del Registro Civil al que se refiere el artículo 2 que se haya incluido en los modelos oficialmente aprobados. Si la madre hubiera renunciado a su hijo en el momento del parto el domicilio de la misma estará sujeto al régimen de publicidad restringida, y no figurará a efectos estadísticos.

Artículo 50. *Derecho al nombre.*

1. Toda persona tiene derecho a un nombre desde su nacimiento.

2. Las personas son identificadas por su nombre y apellidos.

3. El Encargado impondrá un nombre y unos apellidos de uso corriente al nacido cuya filiación sea desconocida. Igualmente impondrá, tras haberles apercibido y transcurrido un plazo de tres días, un nombre de uso corriente cuando los obligados a su fijación no lo señalaren.

4. A petición del interesado o de su representante legal, el encargado del Registro sustituirá el nombre propio de aquél por su equivalente en cualquiera de las lenguas españolas.

Artículo 51. *Principio de libre elección del nombre propio.*

El nombre propio será elegido libremente y sólo quedará sujeto a las siguientes limitaciones, que se interpretarán restrictivamente:

1.º No podrán consignarse más de dos nombres simples o uno compuesto.
2.º No podrán imponerse nombres que sean contrarios a la dignidad de la persona ni los que hagan confusa la identificación.
3.º No podrá imponerse al nacido nombre que ostente uno de sus hermanos con idénticos apellidos, a no ser que hubiera fallecido.

Artículo 52. *Cambio de nombre.*

El Encargado del Registro Civil, mediante procedimiento registral, podrá autorizar el cambio de nombre previa declaración del interesado, que deberá probar el uso habitual del nuevo nombre, y siempre que concurran las demás circunstancias exigidas en la legislación del Registro Civil.

Artículo 53. *Cambio de apellidos mediante declaración de voluntad.*

El Encargado puede, mediante declaración de voluntad del interesado, autorizar el cambio de apellidos en los casos siguientes:

1.º La inversión del orden de apellidos.
2.º La anteposición de la preposición «de» al primer apellido que fuera usualmente nombre propio o empezare por tal, así como las conjunciones «y» o «i» entre los apellidos.
3.º La acomodación de los apellidos de los hijos mayores de edad o emancipados al cambio de apellidos de los padres cuando aquellos expresamente lo consientan.
4.º La regularización ortográfica de los apellidos a cualquiera de las lenguas oficiales correspondiente al origen o domicilio del interesado y la adecuación gráfica a dichas lenguas de la fonética de apellidos también extranjeros.
5.º Cuando sobre la base de una filiación rectificada con posterioridad, el hijo o sus descendientes pretendieran conservar los apellidos que vinieren usando antes de la rectificación. Dicha conservación de apellidos deberá instarse dentro de los dos meses siguientes a la inscripción de la nueva filiación o, en su caso, a la mayoría de edad.

Artículo 54. *Cambio de apellidos o de identidad mediante expediente.*

1. El Encargado del Registro puede autorizar el cambio de apellidos, previo expediente instruido en forma reglamentaria.
2. Son requisitos necesarios de la petición de cambio de apellidos:

a) Que el apellido en la forma propuesta constituya una situación de hecho, siendo utilizado habitualmente por el interesado.
b) Que el apellido o apellidos que se tratan de unir o modificar pertenezcan legítimamente al peticionario.
c) Que los apellidos que resulten del cambio no provengan de la misma línea.

Podrá formularse oposición fundada únicamente en el incumplimiento de los requisitos exigidos.
3. Bastará que concurra el requisito del uso habitual del apellido propuesto, sin que se cumplan los requisitos b) y c) del apartado 2, si el apellido o apellidos solicitados correspondieran a quien tuviere acogido al interesado, siempre que aquél o, por haber fallecido, sus herederos den su consentimiento al cambio. En todo caso se requiere que, por sí o sus representantes legales, asientan al cambio el cónyuge y descendientes del titular del apellido.
4. No será necesario que concurra el uso habitual del apellido propuesto, bastando que se cumplan los requisitos b) y c) previstos en el apartado 2, para cambiar o modificar un apellido contrario a la dignidad o que ocasione graves inconvenientes.
5. Cuando se trate de víctimas de violencia de género o de sus descendientes que estén o hayan estado integrados en el núcleo familiar de convivencia, podrá autorizarse el cambio

de apellidos sin necesidad de cumplir con los requisitos previstos en el apartado 2, de acuerdo con el procedimiento que se determine reglamentariamente.

En estos casos, podrá autorizarse por razones de urgencia o seguridad el cambio total de identidad sin necesidad de cumplir con los requisitos previstos en el apartado 2, de acuerdo con el procedimiento que se determine reglamentariamente.

Artículo 55. *Autorización del cambio de apellidos o identidad en circunstancias excepcionales.*

Cuando razones de urgencia o seguridad no contempladas en el artículo 54.5 u otras circunstancias excepcionales lo requieran, podrá autorizarse el cambio de apellidos o el cambio total de identidad, por Orden del Ministerio de Justicia, en los términos fijados reglamentariamente.

Artículo 56. *Apellidos con elemento extranjero.*

El que adquiere la nacionalidad española conservará los apellidos que ostente en forma distinta de la legal, siempre que así lo declare en el acto de adquirirla o dentro de los dos meses siguientes a la adquisición o a la mayoría de edad, y que los apellidos que se pretenden conservar no resulten contrarios al orden público internacional.

En caso de ciudadanos españoles que tengan igualmente la nacionalidad de otro Estado miembro de la Unión Europea, los cambios de apellidos voluntarios realizados de conformidad con las reglas relativas a la determinación de apellidos aplicables en este último Estado serán reconocidos en España, salvo cuando dicho cambio sea contrario al orden público español, o bien cuando habiendo sido dicho cambio resultado de una resolución judicial ésta no haya sido reconocida en España.

Artículo 57. *Reglas comunes al cambio de nombre y apellidos.*

1. El cambio de apellidos alcanza a todas las personas sujetas a la patria potestad y también a los demás descendientes que expresamente lo consientan.
2. El cambio de nombre y apellidos se inscribirá en el registro individual del interesado. Dicha inscripción tiene carácter constitutivo.
3. Los cambios señalados en los párrafos anteriores podrán ser solicitados por el propio interesado si es mayor de dieciséis años.

CAPÍTULO SEGUNDO

Inscripciones relativas al matrimonio

Artículo 58. *Procedimiento de autorización matrimonial.*

1. El matrimonio en forma civil se celebrará ante el Juez de Paz, Alcalde o Concejal en quien éste delegue, Secretario judicial, Notario, o funcionario diplomático o consular Encargado del Registro Civil.
2. La celebración del matrimonio requerirá la previa tramitación o instrucción de un acta o expediente a instancia de los contrayentes para acreditar el cumplimiento de los requisitos de capacidad y la inexistencia de impedimentos o su dispensa, o cualquier otro obstáculo, de acuerdo con lo previsto en el Código Civil. La tramitación del acta competerá al Notario del lugar del domicilio de cualquiera de los contrayentes. La instrucción del expediente corresponderá al Secretario judicial o Encargado del Registro Civil del domicilio de uno de los contrayentes.
3. El procedimiento finalizará con una resolución en la que se autorice o deniegue la celebración del matrimonio. La denegación deberá ser motivada y expresar, en su caso, con claridad la falta de capacidad o el impedimento en el que se funda la denegación.
4. Contra esta resolución cabe recurso ante el Encargado del Registro Civil, cuya resolución se someterá al régimen de recursos ante la Dirección General de los Registros y del Notariado previsto por esta Ley.
5. El Letrado de la Administración de Justicia, Notario o Encargado del Registro Civil oirá a ambos contrayentes reservadamente y por separado para cerciorarse de su capacidad y

de la inexistencia de cualquier impedimento. Asimismo, se podrán solicitar los informes y practicar las diligencias pertinentes, sean o no propuestas por los requirentes, para acreditar el estado, capacidad o domicilio de los contrayentes o cualesquiera otros extremos necesarios para apreciar la validez de su consentimiento y la veracidad del matrimonio.

El Letrado de la Administración de Justicia, Notario, Encargado del Registro Civil o funcionario que tramite el acta o expediente, cuando sea necesario, podrá recabar de las Administraciones o entidades de iniciativa social de promoción y protección de los derechos de las personas con discapacidad, la provisión de apoyos humanos, técnicos y materiales que faciliten la emisión, interpretación y recepción del consentimiento del o los contrayentes. Solo en el caso excepcional de que alguno de los contrayentes presentare una condición de salud que, de modo evidente, categórico y sustancial, pueda impedirle prestar el consentimiento matrimonial pese a las medidas de apoyo, se recabará dictamen médico sobre su aptitud para prestar el consentimiento.

De la realización de todas estas actuaciones se dejará constancia en el acta o expediente, archivándose junto con los documentos previos a la inscripción de matrimonio.

Pasado un año desde la publicación de los anuncios o de las diligencias sustitutorias sin que se haya contraído el matrimonio, no podrá celebrarse este sin nueva publicación o diligencias.

6. Realizadas las anteriores diligencias, el Secretario judicial, Notario o Encargado del Registro Civil que haya intervenido finalizará el acta o dictará resolución haciendo constar la concurrencia o no en los contrayentes de los requisitos necesarios para contraer matrimonio, así como la determinación del régimen económico matrimonial que resulte aplicable y, en su caso, la vecindad civil de los contrayentes, entregando copia a éstos. La actuación o resolución deberá ser motivada y expresar, en su caso, con claridad la falta de capacidad o el impedimento que concurra.

7. Si el juicio del Secretario judicial, Notario o Encargado del Registro Civil fuera desfavorable se procederá al cierre del acta o expediente y los interesados podrán recurrir ante la Dirección General de los Registros y del Notariado, sometiéndose al régimen de recursos previsto por esta Ley.

8. Resuelto favorablemente el expediente por el Secretario judicial, el matrimonio se podrá celebrar ante el mismo u otro Secretario judicial, Juez de Paz, Alcalde o Concejal en quien éste delegue, a elección de los contrayentes. Si se hubiere tramitado por el Encargado del Registro Civil, el matrimonio deberá celebrarse ante el Juez de Paz, Alcalde o Concejal en quien éste delegue, que designen los contrayentes. Finalmente, si fuera el Notario quien hubiera extendido el acta matrimonial, los contrayentes podrán otorgar el consentimiento, a su elección, ante el mismo Notario u otro distinto del que hubiera tramitado el acta previa, el Juez de Paz, Alcalde o Concejal en quien éste delegue. La prestación del consentimiento deberá realizarse en la forma prevista en el Código Civil.

El matrimonio celebrado ante Juez de Paz, Alcalde o Concejal en quien este delegue o ante el Secretario judicial se hará constar en acta; el que se celebre ante Notario constará en escritura pública. En ambos casos deberá ser firmada, además de por aquel ante el que se celebra, por los contrayentes y dos testigos.

Extendida el acta o autorizada la escritura pública, se entregará a cada uno de los contrayentes copia acreditativa de la celebración del matrimonio y se remitirá por el autorizante, en el mismo día y por medios telemáticos, testimonio o copia autorizada electrónica del documento al Registro Civil para su inscripción, previa calificación del Encargado del Registro Civil.

9. La celebración del matrimonio fuera de España corresponderá al funcionario consular o diplomático Encargado del Registro Civil en el extranjero. Si uno o los dos contrayentes residieran en el extranjero, la tramitación del expediente previo podrá corresponder al funcionario diplomático o consular Encargado del registro civil competente en la demarcación consular donde residan. El matrimonio así tramitado podrá celebrarse ante el mismo funcionario u otro distinto, o ante el Juez de Paz, Alcalde o Concejal en quien éste delegue, a elección de los contrayentes.

10. Cuando el matrimonio se hubiere celebrado sin haberse tramitado el correspondiente expediente o acta previa, si éste fuera necesario, el Secretario judicial, Notario, o el funcionario Encargado del Registro Civil que lo haya celebrado, antes de realizar las

actuaciones que procedan para su inscripción, deberá comprobar si concurren los requisitos legales para su validez, mediante la tramitación del acta o expediente al que se refiere este artículo.

Si la celebración del matrimonio hubiera sido realizada ante autoridad o persona competente distinta de las indicadas en el párrafo anterior, el acta de aquélla se remitirá al Encargado del Registro Civil del lugar de celebración para que proceda a la comprobación de los requisitos de validez, mediante el expediente correspondiente. Efectuada esa comprobación, el Encargado del Registro Civil procederá a su inscripción.

12 [sic]. Si los contrayentes hubieran manifestado su propósito de contraer matrimonio en el extranjero, con arreglo a la forma establecida por la ley del lugar de celebración o en forma religiosa y se exigiera la presentación de un certificado de capacidad matrimonial, lo expedirá el Secretario judicial, Notario, Encargado del Registro Civil o funcionario consular o diplomático del lugar del domicilio de cualquiera de los contrayentes, previo expediente instruido o acta que contenga el juicio del autorizante acreditativo de la capacidad matrimonial de los contrayentes.

Artículo 58 bis. *Matrimonio celebrado en forma religiosa.*

1. Para la celebración del matrimonio en la forma religiosa prevista en el Acuerdo entre el Estado español y la Santa Sede sobre Asuntos Jurídicos y en los Acuerdos de cooperación del Estado con las confesiones religiosas se estará a lo dispuesto en los mismos.

2. En los supuestos de celebración del matrimonio en la forma religiosa prevista por las iglesias, confesiones, comunidades religiosas o federaciones de las mismas que, inscritas en el Registro de Entidades Religiosas, hayan obtenido el reconocimiento de notorio arraigo en España, requerirán la tramitación de un acta o expediente previo de capacidad matrimonial conforme al artículo anterior. Cumplido este trámite, el Secretario judicial, Notario, Encargado del Registro Civil o funcionario diplomático o consular Encargado del Registro Civil que haya intervenido expedirá dos copias del acta o resolución, que incluirá, en su caso, el juicio acreditativo de la capacidad matrimonial de los contrayentes, que éstos deberán entregar al ministro de culto encargado de la celebración del matrimonio.

El consentimiento deberá prestarse ante un ministro de culto y dos testigos mayores de edad. En estos casos, el consentimiento deberá prestarse antes de que hayan transcurrido seis meses desde la fecha del acta o resolución que contenga el juicio de capacidad matrimonial. A estos efectos se consideran ministros de culto a las personas físicas dedicadas, con carácter estable, a las funciones de culto o asistencia religiosa y que acrediten el cumplimiento de estos requisitos mediante certificación expedida por la iglesia, confesión o comunidad religiosa que haya obtenido el reconocimiento de notorio arraigo en España, con la conformidad de la federación que en su caso hubiera solicitado dicho reconocimiento.

Una vez celebrado el matrimonio, el oficiante extenderá certificación expresiva de la celebración del mismo, con los requisitos necesarios para su inscripción y las menciones de identidad de los testigos y de las circunstancias del expediente o acta previa que necesariamente incluirán el nombre y apellidos del Secretario judicial, Notario, Encargado del Registro Civil o funcionario diplomático o consular que la hubiera extendido, la fecha y número de protocolo en su caso. Esta certificación se remitirá por medios electrónicos, en la forma que reglamentariamente se determine, junto con la certificación acreditativa de la condición de ministro de culto, dentro del plazo de cinco días al Encargado del Registro Civil competente para su inscripción. Igualmente extenderá en las dos copias del acta o resolución previa de capacidad matrimonial diligencia expresiva de la celebración del matrimonio entregando una a los contrayentes y conservará la otra como acta de la celebración en el archivo del oficiante o de la entidad religiosa a la que representa como ministro de culto.

Artículo 59. *Inscripción del matrimonio.*

1. El matrimonio cuyos requisitos se hayan constatado y celebrado según el procedimiento previsto en el artículo 58 se inscribirá en los registros individuales de los contrayentes.

2. El matrimonio celebrado ante autoridad extranjera accederá al Registro Civil español mediante la inscripción de la certificación correspondiente, siempre que tenga eficacia con arreglo a lo previsto en la presente Ley.

3. El matrimonio celebrado en España en forma religiosa accederá al Registro Civil mediante la inscripción de la certificación emitida por el ministro de culto, conforme a lo previsto en el artículo 63 del Código Civil.

4. Practicada la inscripción, el Encargado del Registro Civil pondrá a disposición de cada uno de los contrayentes certificación de la inscripción del matrimonio.

5. La inscripción hace fe del matrimonio y de la fecha y lugar en que se contrae y produce el pleno reconocimiento de los efectos civiles del mismo frente a terceros de buena fe.

Artículo 60. *Inscripción del régimen económico del matrimonio.*

1. Junto a la inscripción de matrimonio se inscribirá el régimen económico matrimonial legal o pactado que rija el matrimonio y los pactos, resoluciones judiciales o demás hechos que puedan afectar al mismo.

2. Cuando no se presenten escrituras de capitulaciones se inscribirá como régimen económico matrimonial legal el que fuera supletorio de conformidad con la legislación aplicable. Para hacer constar en el Registro Civil expresamente el régimen económico legal aplicable a un matrimonio ya inscrito cuando aquél no constase con anterioridad y no se aporten escrituras de capitulaciones será necesaria la tramitación de un acta de notoriedad.

Otorgada ante Notario escritura de capitulaciones matrimoniales, deberá éste remitir en el mismo día copia autorizada electrónica de la escritura pública al Encargado del Registro Civil correspondiente para su constancia en la inscripción de matrimonio. Si el matrimonio no se hubiera celebrado a la fecha de recepción de la escritura de capitulaciones matrimoniales, el Encargado del Registro procederá a su anotación en el registro individual de cada contrayente.

3. En las inscripciones que en cualquier otro Registro produzcan las capitulaciones y demás hechos que afecten al régimen económico matrimonial, se expresarán los datos de su inscripción en el Registro Civil.

4. Sin perjuicio de lo previsto en el artículo 1333 del Código Civil, en ningún caso el tercero de buena fe resultará perjudicado sino desde la fecha de la inscripción del régimen económico matrimonial o de sus modificaciones.

Artículo 61. *Inscripción de la separación, nulidad y divorcio.*

El letrado de la Administración de Justicia del juzgado o tribunal que hubiera dictado la resolución judicial firme de separación, nulidad o divorcio deberá remitir en el mismo día o al siguiente hábil y por medios electrónicos testimonio o copia electrónica de la misma a la Oficina General del Registro Civil, la cual practicará de forma inmediata la correspondiente inscripción. Las resoluciones judiciales que resuelvan sobre la nulidad, separación y divorcio podrán ser objeto de anotación hasta que adquieran firmeza.

La misma obligación tendrá el notario que hubiera autorizado la escritura pública formalizando un convenio regulador de separación o divorcio.

Las resoluciones judiciales o las escrituras públicas que modifiquen las inicialmente adoptadas o convenidas también deberán ser inscritas en el Registro Civil.

Las resoluciones sobre disolución de matrimonio canónico, dictadas por autoridad eclesiástica reconocida, se inscribirán si cumplen los requisitos que prevé el ordenamiento jurídico.

CAPÍTULO TERCERO

Inscripción de la defunción

Artículo 62. *Inscripción de la defunción.*

1. La inscripción en el Registro Civil de la defunción es obligatoria. La inscripción hace fe de la muerte de una persona y de la fecha, hora y lugar en que se produce. En la inscripción debe figurar asimismo la identidad del fallecido.

2. La inscripción de la defunción se practicará en virtud de declaración documentada en el formulario oficial, acompañado del certificado médico de la defunción. En defecto de certificado, cuando éste sea incompleto o si, a juicio del Encargado, debe complementarse la documentación acreditativa del fallecimiento, se requerirá dictamen médico del facultativo.

3. El funcionario competente, una vez recibida y examinada la documentación, practicará inmediatamente la inscripción y expedirá el certificado de la defunción.

El Encargado, una vez practicada la inscripción, expedirá la licencia para el entierro o incineración en el plazo que reglamentariamente se establezca.

4. La inscripción de la defunción cerrará el registro individual. En ningún caso, el código personal podrá volver a ser asignado.

Artículo 63. *Obligados a promover la inscripción de fallecimiento.*

Están obligados a promover la inscripción de fallecimiento:

1.º La dirección de hospitales, clínicas y establecimientos sanitarios donde se produzca el fallecimiento.

2.º El personal médico que certifica el fallecimiento, cuando éste haya tenido lugar fuera del establecimiento sanitario.

3.º Los parientes del difunto o persona a quien éstos autoricen.

4.º El director del establecimiento, cualquier habitante de la casa donde se hubiera producido el fallecimiento o, en su caso, la autoridad que corresponda.

5.º Cualquier persona que tenga conocimiento de un fallecimiento lo comunicará a la autoridad competente, que vendrá obligada a promover la inscripción de la defunción.

Artículo 64. *Comunicación de la defunción por los centros sanitarios.*

La dirección de hospitales, clínicas y establecimientos sanitarios comunicará a la Oficina del Registro Civil competente y al Instituto Nacional de Estadística cada uno de los fallecimientos que hayan tenido lugar en su centro sanitario. La comunicación se remitirá por medios electrónicos en el plazo que se establezca reglamentariamente mediante el envío del formulario oficial debidamente cumplimentado, acompañado del certificado médico firmado por el facultativo. Dicha remisión será realizada por personal del centro sanitario, que usará para ello mecanismos seguros de identificación y firma electrónicos.

Artículo 65. *Inscripción de la defunción por declaración de los obligados.*

Respecto de los fallecimientos que se hayan producido fuera de establecimiento sanitario, los obligados a promover la inscripción informarán de la defunción a la mayor brevedad posible a la autoridad pública, que la comunicará inmediatamente a la Oficina del Registro Civil.

Artículo 66. *Certificado médico de defunción.*

En ningún caso podrá efectuarse la inscripción de defunción sin que se haya presentado ante el Registro Civil el certificado médico de defunción. En el certificado, además de las circunstancias necesarias para la práctica de la inscripción, deberán recogerse aquellas que se precisen a los fines del Instituto Nacional de Estadística y, en todo caso, la existencia o no de indicios de muerte violenta y, en su caso, la incoación o no de diligencias judiciales por el fallecimiento si le fueran conocidas o cualquier motivo por el que, a juicio del facultativo, no deba expedirse la licencia de enterramiento.

Las circunstancias mencionadas en el segundo inciso del párrafo anterior no serán incorporadas a la inscripción de defunción ni serán objeto del régimen de publicidad establecido en esta Ley, siendo su única finalidad la establecida en este artículo.

Artículo 67. *Supuestos especiales de inscripción de la defunción.*

1. Cuando el cadáver hubiera desaparecido o se hubiera inhumado antes de la inscripción, será necesaria resolución del Secretario judicial declarando el fallecimiento u orden de la autoridad judicial en la que se acredite legalmente el fallecimiento.

2. Si hubiera indicios de muerte violenta o en cualquier caso en que deban incoarse diligencias judiciales, la inscripción de la defunción no supondrá por sí misma la concesión de licencia de enterramiento o incineración. Dicha licencia se expedirá cuando se autorice por el órgano judicial competente.

3. Cuando el fallecimiento hubiere ocurrido con posterioridad a los seis primeros meses de gestación, antes del nacimiento, y siempre que el recién nacido hubiera fallecido antes de recibir el alta médica, después del parto, el certificado médico deberá ser firmado, al menos, por dos facultativos, quienes afirmarán, bajo su responsabilidad que, del parto y, en su caso, de las pruebas realizadas con el material genético de la madre y el hijo, no se desprenden dudas razonables sobre la relación materno filial; haciéndose constar en la inscripción, o en el archivo a que se refiere la disposición adicional cuarta en su caso, la realización de dichas pruebas y el centro sanitario que inicialmente conserve la información relacionada con las mismas, sin perjuicio del traslado de esta información a los archivos definitivos de la Administración correspondiente cuando proceda.

CAPÍTULO CUARTO

Otras inscripciones

Artículo 68. *Inscripción de la nacionalidad y de la vecindad civil.*

1. La adquisición de la nacionalidad española por residencia, carta de naturaleza y opción, así como su recuperación y las declaraciones de voluntad relativas a la vecindad, se inscribirán en el registro individual. Estas inscripciones tendrán carácter constitutivo.

No podrá inscribirse la nacionalidad española adquirida por cualquiera de las vías que reconoce el ordenamiento jurídico si no se ha efectuado la inscripción previa de nacimiento.

La inscripción de la pérdida de la nacionalidad tendrá carácter meramente declarativo.

2. Para efectuar las inscripciones relativas a la nacionalidad y a la vecindad civil será título suficiente aquél a través del cual se haya reconocido la nacionalidad española o la vecindad civil que corresponda.

3. Las declaraciones de voluntad relativas a la adquisición de la nacionalidad española por residencia, carta de naturaleza y opción, así como su recuperación, conservación o pérdida, y las declaraciones de voluntad relativas a la vecindad, podrán realizarse ante el Encargado del Registro Civil, notario, o funcionario diplomático o consular encargado del Registro Civil.

Artículo 69. *Presunción de nacionalidad española.*

Sin perjuicio de lo dispuesto en el Código Civil y en tanto no conste la extranjería de los padres, se presumen españoles los nacidos en territorio español de padres también nacidos en España.

La misma presunción rige para la vecindad.

Artículo 70. *Emancipación y beneficio de la mayor edad.*

1. En el registro individual se inscribirán la emancipación y el beneficio de la mayor edad.

2. La emancipación por concesión de los que ejercen la patria potestad se inscribe en virtud de escritura pública o por comparecencia ante el Encargado.

3. La emancipación por concesión judicial y el beneficio de la mayor edad se inscriben en virtud de resolución judicial.

4. La emancipación tácita o por vida independiente podrá inscribirse mediante la acreditación documental de la situación de independencia y el consentimiento de quienes ejercen la patria potestad.

La concesión de emancipación y la emancipación por vida independiente, así como el beneficio de la mayor edad, no producirán efectos frente a terceros mientras no se inscriban en el Registro Civil.

Artículo 71. *Inscripción de la patria potestad y sus modificaciones.*

1. Los hechos que afecten a las relaciones paterno-filiales se inscribirán en el registro individual de la persona sujeta a patria potestad y en el de su progenitor o en los de sus progenitores.

Son inscribibles las resoluciones judiciales que afecten a la titularidad, al ejercicio y a las modificaciones de la patria potestad. En particular, las que se produzcan como consecuencia de la nulidad, separación y divorcio de los progenitores.

2. También se inscribirá la extinción, privación, suspensión y recuperación de la patria potestad.

Téngase en cuenta que esta última actualización del apartado 2 establecida por el art. 6.4 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"2. También se inscribirá la extinción, privación, suspensión, prórroga y rehabilitación de la patria potestad."

3. En idénticos términos se inscribirá todo lo relativo a las figuras similares o asimilables a la patria potestad, que sean de Derecho civil propio de las Comunidades Autónomas.

Artículo 72. *Resolución judicial de provisión de apoyos y declaración del concurso de persona física.*

1. La resolución judicial dictada en un procedimiento de provisión de apoyos, así como la que la deje sin efecto o la modifique, se inscribirán en el registro individual de la persona con discapacidad. La inscripción expresará la extensión y límites de las medidas judiciales de apoyo.

Asimismo, se inscribirá cualquier otra resolución judicial sobre las medidas de apoyo a personas con discapacidad.»

Téngase en cuenta que esta última actualización del título y del apartado 1 establecida por el art. 6.5 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"**Artículo 72. Modificación judicial de la capacidad y declaración del concurso de persona física.**

1. La declaración judicial de modificación de la capacidad, así como la resolución que la deje sin efecto o la modifique, se inscribirán en el registro individual del afectado."

La inscripción de la modificación judicial de la capacidad expresará la extensión y límites de ésta, así como si la persona queda sujeta a tutela o curatela según la resolución judicial.

2. Se inscribirán en el Registro Civil la declaración de concurso, la intervención o, en su caso, la suspensión de las facultades de administración y disposición, así como el nombramiento de los administradores concursales.

Artículo 73. *Oponibilidad de las resoluciones.*

Las resoluciones a que se refiere el artículo anterior solo serán oponibles frente a terceros cuando se hayan practicado las oportunas inscripciones.

Téngase en cuenta que esta última actualización establecida por el art. 6.6 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"**Artículo 73. Inscripción de tutela, curatela y sus modificaciones.**

1. Se inscribirán en el registro individual de la persona con capacidad modificada judicialmente las resoluciones judiciales en las que se nombre tutor o curador.

Asimismo, tendrán acceso al Registro Civil las medidas judiciales sobre guarda o administración y sobre vigilancia o control de dichos cargos tutelares.

2. Dichas resoluciones solo serán oponibles frente a terceros cuando se hayan practicado las oportunas inscripciones."

Artículo 74. *Inscripción de determinadas representaciones legales.*

1. Tienen acceso al registro individual la representación del ausente y la designación de defensor judicial en el caso previsto en el artículo 299 bis del Código Civil.

2. Igualmente, podrá tener acceso al Registro Civil cualquier representación que se otorgue mediante nombramiento especial y comprenda la administración y guarda de un patrimonio.

Artículo 75. *Inscripción de tutela automática o administrativa.*

Se inscribirá en el registro individual del menor en situación de desamparo la sujeción a la tutela por la entidad pública a la que, en el respectivo territorio, esté encomendada la protección de los menores por la legislación que resulte aplicable.

Téngase en cuenta que esta última actualización establecida por el art. 6.7 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"**Artículo 75. Inscripción de tutela automática o administrativa.**

Se inscribirá en el registro individual del menor o de la persona con capacidad modificada judicialmente en situación de desamparo, la sujeción a la tutela por la entidad pública a la que, en el respectivo territorio, esté encomendada la protección de los menores o de las personas con capacidad modificada judicialmente en los términos previstos por la legislación que resulte aplicable."

Artículo 76. *Inscripción de actos relativos al patrimonio protegido de las personas con discapacidad.*

Es inscribible en el registro individual de la persona con discapacidad el documento público o resolución judicial relativos a la constitución y demás circunstancias relativas al patrimonio protegido y a la designación y modificación de administradores de dicho patrimonio.

Artículo 77. *Inscripción de medidas de apoyo voluntarias.*

Es inscribible en el registro individual del interesado el documento público que contenga las medidas de apoyo previstas por una persona respecto de sí misma o de sus bienes.

Téngase en cuenta que esta última actualización establecida por el art. 6.8 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"**Artículo 77. Inscripción de autotutela y apoderamientos preventivos.**

Es inscribible en el registro individual del interesado el documento público de constitución de autotutela y el apoderamiento preventivo previstos en la legislación civil."

Artículo 78. *Inscripciones de declaración de ausencia y fallecimiento.*

1. Las declaraciones judiciales de ausencia y fallecimiento se inscribirán en el registro individual del declarado ausente o fallecido.
2. En la inscripción de la declaración de fallecimiento se expresará la fecha a partir de la cual se entiende ocurrida la muerte.
3. En las inscripciones de la declaración de ausencia y fallecimiento se hará constar cuanto se previene en el artículo 198 del Código Civil.

CAPÍTULO QUINTO

Inscripciones en circunstancias excepcionales

Artículo 79. *Inscripciones en circunstancias excepcionales.*

Cuando por circunstancias excepcionales imputables al funcionamiento del Registro Civil no sea posible practicar la inscripción, se levantará acta de nacimiento, matrimonio o defunción con los requisitos del asiento correspondiente por las autoridades o funcionarios que señale el Reglamento.

Dicha acta será título suficiente para proceder a la inscripción del hecho o acto a que se refiere el párrafo anterior con independencia del tiempo transcurrido desde el hecho y sin necesidad de incoar un expediente de inscripción fuera de plazo.

TÍTULO VII

Publicidad del Registro Civil

CAPÍTULO PRIMERO

Instrumentos de publicidad registral

Artículo 80. *Medios de publicidad del Registro Civil.*

1. La publicidad de los datos que constan en el Registro Civil se realizará de las siguientes formas:

1.ª Mediante el acceso de las Administraciones y funcionarios públicos, en el ejercicio de sus funciones y bajo su responsabilidad, a los datos que consten en el Registro Civil.

También se podrá tener conocimiento de los datos que constan en el Registro Civil mediante los procedimientos especiales que se acuerden por la Dirección General de los Registros y del Notariado, cuando la información deba ser suministrada de forma periódica y automatizada para el cumplimiento de fines públicos, o cuando sea precisa para comprobar por las entidades de certificación reguladas en la Ley 59/2003, de 19 de diciembre, de firma

electrónica, que no se ha producido la extinción de los certificados electrónicos por las causas contempladas en el artículo 8, apartado 1, letra e), de dicha Ley.

2.ª Mediante certificación.

2. Las Administraciones y funcionarios públicos en el ejercicio de sus competencias sólo podrán exigir a los ciudadanos la presentación de certificados del Registro Civil cuando los datos objeto del certificado no obren en poder de aquéllas, o cuando fuere imposible su obtención directamente por medios electrónicos.

3. Lo dispuesto en este artículo se entiende sin perjuicio del régimen de publicidad restringida al que se refieren los artículos 83 y 84 de la presente Ley.

4. Con carácter excepcional y con fines de investigación familiar, histórica o científica, se podrá autorizar el acceso a la información registral en los términos que reglamentariamente se establezcan.

Artículo 81. *Expedición de certificaciones.*

1. Son competentes para expedir certificaciones de los datos que consten en los asientos del Registro Civil los Encargados de las Oficinas del Registro Civil.

2. Las certificaciones se expedirán por medios electrónicos. Excepcionalmente, también se podrán expedir por medios no electrónicos. A petición del interesado, las certificaciones podrán ser bilingües.

3. Las certificaciones previstas en el apartado anterior se presumen exactas y constituyen prueba plena de los hechos y actos inscritos en el Registro Civil.

4. Cuando por circunstancias excepcionales la certificación no fuese conforme con los datos que consten en el Registro Civil, se estará a lo que de éste resulte, sin perjuicio de la responsabilidad que proceda.

Artículo 82. *Clases de certificaciones.*

1. Las certificaciones podrán ser literales o en extracto. Salvo solicitud expresa en sentido contrario, se expedirá certificación en extracto. Si no constara ningún asiento, la certificación será negativa.

2. Las certificaciones literales comprenderán la totalidad del contenido del asiento o asientos a que se refieran.

3. Las certificaciones en extracto contendrán los datos que se determinen reglamentariamente.

CAPÍTULO SEGUNDO

Datos sometidos a régimen de protección especial

Artículo 83. *Datos con publicidad restringida.*

1. A los efectos de la presente Ley, se considerarán datos especialmente protegidos:

a) La filiación adoptiva y la desconocida.

b) La discapacidad y las medidas de apoyo.

c) Los cambios de apellido autorizados por ser víctima de violencia de género o su descendiente, así como otros cambios de identidad legalmente autorizados.

d) La rectificación del sexo.

e) Las causas de privación o suspensión de la patria potestad.

f) El matrimonio secreto.

Téngase en cuenta que esta última actualización del apartado 1 establecida por el art. 6.9 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:

"1. A los efectos de la presente Ley, se considerarán datos especialmente protegidos:

a) La filiación adoptiva y la desconocida.
b) Los cambios de apellido autorizados por ser víctima de violencia de género o su descendiente, así como otros cambios de identidad legalmente autorizados.
c) La rectificación del sexo.
d) Las causas de privación o suspensión de la patria potestad.
e) El matrimonio secreto."

2. Estarán sometidos al mismo régimen de protección los documentos archivados por contener los extremos citados en el apartado anterior o que estén incorporados a expedientes que tengan carácter reservado.

3. Los asientos que contengan información relativa a los datos relacionados en el apartado anterior serán efectuados del modo que reglamentariamente se determine con el fin de que, salvo el propio inscrito, solo se pueda acceder a ellos con la autorización expresada en el artículo siguiente.

Artículo 84. *Acceso a los asientos que contengan datos especialmente protegidos.*

Sólo el inscrito o sus representantes legales, quien ejerza el apoyo y que esté expresamente autorizado, el apoderado preventivo general o el curador en el caso de una persona con discapacidad podrán acceder o autorizar a terceras personas la publicidad de los asientos que contengan datos especialmente protegidos en los términos que reglamentariamente se establezcan. Las Administraciones Públicas y los funcionarios públicos podrán acceder a los datos especialmente protegidos del apartado 1.b) del artículo 83 cuando en el ejercicio de sus funciones deban verificar la existencia o el contenido de medidas de apoyo.

Téngase en cuenta que esta última actualización del párrafo primero establecida por el art. 6.10 de la Ley 8/2021, de 2 de junio. Ref. BOE-A-2021-9233, entra en vigor el 3 de septiembre de 2021, según determina su disposición final 3.

Redacción anterior:
"Sólo el inscrito o sus representantes legales podrán acceder o autorizar a terceras personas la publicidad de los asientos que contengan datos especialmente protegidos en los términos que reglamentariamente se establezcan."

Si el inscrito ha fallecido, la autorización para acceder a los datos especialmente protegidos sólo podrá efectuarla el Juez de Primera Instancia del domicilio del solicitante, siempre que justifique interés legítimo y razón fundada para pedirlo.

En el supuesto del párrafo anterior, se presume que ostenta interés legítimo el cónyuge del fallecido, pareja de hecho, ascendientes y descendientes hasta el segundo grado.

TÍTULO VIII

Régimen de recursos

Artículo 85. *Recursos contra las decisiones adoptadas por los Encargados de las Oficinas del Registro Civil.*

1. Contra las decisiones adoptadas por los Encargados de las Oficinas Central, Generales y Consulares del Registro Civil en el ámbito de las competencias atribuidas por esta Ley, los interesados sólo podrán interponer recurso ante la Dirección General de los Registros y del Notariado, en el plazo de un mes.

2. En el caso de denegación de inscripción de sentencias y otras resoluciones judiciales extranjeras cuya competencia corresponde a la Oficina Central del Registro Civil, el interesado sólo podrá instar procedimiento judicial de *exequátur.*

Artículo 86. *Presentación del recurso y plazo de resolución.*

1. El recurso se dirigirá a la Dirección General de Seguridad Jurídica y Fe Pública y se formulará en los términos previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

El interesado podrá presentar el recurso en cualquiera de los lugares previstos para la presentación de escritos y solicitudes haciendo uso de los medios que prevé el ordenamiento jurídico.

2. La Dirección General resolverá el recurso en el plazo de seis meses siguientes a la recepción del escrito de interposición.

Transcurrido este plazo sin que la Dirección General de Seguridad Jurídica y Fe Pública haya dictado y notificado resolución expresa, se entenderá desestimada la pretensión, quedando expedita la vía jurisdiccional correspondiente.

Artículo 87. *Órgano jurisdiccional competente.*

1. Las resoluciones y actos de la Dirección General de los Registros y del Notariado podrán ser impugnados ante el Juzgado de Primera Instancia de la capital de provincia del domicilio del recurrente, de conformidad con lo previsto en el artículo 781 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. En estos procesos será emplazada la citada Dirección General a través de su representación procesal.

2. Quedan exceptuados del número anterior las resoluciones y actos de la Dirección General de los Registros y del Notariado relativos a la solicitud de nacionalidad por residencia que en aplicación del artículo 22.5 del Código civil se someten a la jurisdicción contencioso-administrativa.

3. La Dirección General de los Registros y del Notariado podrá impugnar ante el Juzgado de Primera Instancia competente las decisiones adoptadas por los Encargados de las Oficinas por ser las mismas contrarias a la doctrina establecida por el Centro Directivo. En estos procesos serán emplazados los interesados.

TÍTULO IX

Los procedimientos registrales

CAPÍTULO PRIMERO

Reglas generales de los procedimientos registrales

Artículo 88. *Tramitación de los procedimientos registrales.*

1. Los procedimientos registrales serán tramitados y resueltos por el Encargado del Registro Civil de la Oficina donde se pretendiera efectuar el asiento. Los procedimientos de rectificación de asientos se tramitarán por el Encargado de la Oficina que los hubiese practicado.

2. La tramitación del procedimiento se ajustará a las reglas previstas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en los términos que reglamentariamente se dispongan. El silencio administrativo en los procedimientos registrales será negativo.

Artículo 89. *Legitimación para promover los procedimientos registrales.*

Además del Ministerio Fiscal, pueden promover los procedimientos registrales quienes estuvieran obligados a promover la inscripción y cualquier persona que tenga interés en los asientos.

CAPÍTULO SEGUNDO

Rectificación de los asientos del Registro Civil

Artículo 90. *Rectificación judicial de los asientos.*

Los asientos están bajo la salvaguarda de los Tribunales y su rectificación se efectuará en virtud de resolución judicial firme de conformidad con lo previsto en el artículo 781 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Artículo 91. *Rectificación de los asientos por procedimiento registral.*

1. No obstante lo previsto en el artículo anterior, pueden rectificarse a través de un procedimiento registral:

a) Las menciones erróneas de los datos que deban constar en la inscripción.
b) Los errores que proceden de documento público o eclesiástico ulteriormente rectificado.
c) Las divergencias que se aprecien entre la inscripción y los documentos en cuya virtud se haya practicado.

2. La mención registral relativa al nombre y sexo de las personas cuando se cumplan los requisitos del artículo 4 de la Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral relativa al sexo de las personas, se rectificará mediante procedimiento registral. En tales casos, la inscripción tendrá eficacia constitutiva.

CAPÍTULO TERCERO

Declaraciones con valor de simple presunción

Artículo 92. *Declaraciones con valor de simple presunción.*

1. Previo procedimiento registral, puede declararse con valor de simple presunción:

a) Que no ha ocurrido hecho determinado que pudiera afectar al estado civil.
b) La nacionalidad, vecindad civil o cualquier estado, si no consta en el Registro Civil.
c) El domicilio de los apátridas.
d) La existencia de los hechos mientras por fuerza mayor sea imposible el acceso a la información contenida en el Registro Civil.
e) El matrimonio cuya celebración conste y que no pueda ser inscrito por no haberse acreditado debidamente los requisitos exigidos para su validez por el Código Civil.

2. La acreditación de las circunstancias referidas en el apartado anterior se efectuará en los términos que reglamentariamente se determinen.

Artículo 93. *Carácter, anotación y publicidad de las declaraciones con valor de simple presunción.*

1. Las declaraciones con valor de simple presunción tienen la consideración de una presunción legal *iuris tantum.*
2. La anotación de las declaraciones es obligatoria y precisará la fecha a que éstas se refieren.
3. El testimonio, literal o en extracto, de las declaraciones expresará siempre su valor de simple presunción.
La publicidad de las anotaciones y declaraciones queda sujeta a las mismas restricciones que la presente Ley prevé para las inscripciones.

TÍTULO X

Normas de Derecho internacional privado

Artículo 94. *Primacía del Derecho convencional y de la Unión Europea.*

Las normas del presente Título se aplicarán sin perjuicio de lo que dispongan la normativa de la Unión Europea y los tratados e instrumentos internacionales vigentes en España.

Artículo 95. *Traducción y legalización.*

1. Los documentos no redactados en una de las lenguas oficiales españolas o escritos en letra antigua o poco inteligible, deberán acompañarse de traducción efectuada por órgano o funcionario competentes. No obstante, si al Encargado del Registro le constare el contenido del documento podrá prescindir de la traducción.
2. Todo documento expedido por funcionario o autoridad extranjera se presentará con la correspondiente legalización. No obstante, quedan eximidos de legalización los documentos cuya autenticidad le constare al Encargado del Registro y aquéllos que llegaren por vía oficial o por diligencia bastante.
3. El Encargado que dude de la autenticidad de un documento, realizará las comprobaciones oportunas en el menor tiempo posible.

Artículo 96. *Resoluciones judiciales extranjeras.*

1. Sólo procederá la inscripción en el Registro Civil español de las sentencias y demás resoluciones judiciales extranjeras que hayan adquirido firmeza. Tratándose de resoluciones de jurisdicción voluntaria, éstas deberán ser definitivas. En el caso de que la resolución carezca de firmeza o de carácter definitivo, únicamente procederá su anotación registral en los términos previstos en el ordinal 5.º del apartado 3 del artículo 40 de la presente Ley.
2. La inscripción de las resoluciones judiciales extranjeras se podrá instar:

1.º Previa superación del trámite del *exequátur* contemplado en la Ley de Enjuiciamiento Civil de 1881. Hasta entonces sólo podrán ser objeto de anotación en los términos previstos en el ordinal 5º del apartado 3 del artículo 40 de la presente Ley.
2.º Ante el Encargado del Registro Civil, quien procederá a realizarla siempre que verifique:

a) La regularidad y autenticidad formal de los documentos presentados.
b) Que el Tribunal de origen hubiera basado su competencia judicial internacional en criterios equivalentes a los contemplados en la legislación española.
c) Que todas las partes fueron debidamente notificadas y con tiempo suficiente para preparar el procedimiento.
d) Que la inscripción de la resolución no resulta manifiestamente incompatible con el orden público español.

El Encargado del Registro Civil deberá notificar su resolución a todos los interesados y afectados por la misma. Contra la resolución del Encargado del Registro Civil los interesados y los afectados podrán solicitar *exequátur* de la resolución judicial o bien interponer recurso ante la Dirección General de los Registros y del Notariado en los términos previstos en la presente Ley. En ambos casos se procederá a la anotación de la resolución en los términos previstos en el ordinal 5º del apartado 3 del artículo 40, si así se solicita expresamente.
3. El régimen jurídico contemplado en el presente artículo para las resoluciones judiciales extranjeras será aplicable a las resoluciones pronunciadas por autoridades no judiciales extranjeras en materias cuya competencia corresponda, según el Derecho español, al conocimiento de Jueces y Tribunales.

Artículo 97. *Documento extranjero extrajudicial.*

Un documento público extranjero no judicial es título para inscribir el hecho o acto de que da fe siempre que cumpla los siguientes requisitos:

1.º Que el documento ha sido otorgado por autoridad extranjera competente conforme a la legislación de su Estado.

2.º Que la autoridad extranjera haya intervenido en la confección del documento desarrollando funciones equivalentes a las que desempeñan las autoridades españolas en la materia de que se trate.

3.º Que el hecho o acto contenido en el documento sea válido conforme al ordenamiento designado por las normas españolas de Derecho internacional privado.

4.º Que la inscripción del documento extranjero no resulte manifiestamente incompatible con el orden público español.

Artículo 98. *Certificación de asientos extendidos en Registros extranjeros.*

1. La certificación de asientos extendidos en Registros extranjeros es título para la inscripción en el Registro Civil español siempre que se verifiquen los siguientes requisitos:

a) Que la certificación ha sido expedida por autoridad extranjera competente conforme a la legislación de su Estado.

b) Que el Registro extranjero de procedencia tenga, en cuanto a los hechos de que da fe, análogas garantías a las exigidas para la inscripción por la ley española.

c) Que el hecho o acto contenido en la certificación registral extranjera sea válido conforme al ordenamiento designado por las normas españolas de Derecho internacional privado.

d) Que la inscripción de la certificación registral extranjera no resulta manifiestamente incompatible con el orden público español.

2. En el caso de que la certificación constituya mero reflejo registral de una resolución judicial previa, será ésta el título que tenga acceso al Registro. Con tal fin, deberá reconocerse la resolución judicial de acuerdo a alguno de los procedimientos contemplados en el artículo 96 de la presente Ley.

3. Se completarán por los medios legales o convencionales oportunos los datos y circunstancias que no puedan obtenerse directamente de la certificación extranjera, por no contenerlos o por defectos formales que afecten a la autenticidad o a la realidad de los hechos que incorporan.

Artículo 99. *Declaración de conocimiento o voluntad.*

1. Los hechos y actos que afecten al estado civil de las personas y cuyo acceso al Registro Civil se realice mediante declaración de conocimiento o voluntad, deberán ajustarse a su correspondiente ordenamiento aplicable, determinado conforme a las normas españolas de Derecho internacional privado.

2. Sin perjuicio de lo contenido en el número anterior, el acceso al Registro de hechos y actos relativos al estado de las personas a través de declaración de conocimiento o voluntad se llevará a cabo en los casos, formas, procedimientos y modalidades establecidos en esta Ley.

Artículo 100. *Acreditación del contenido y vigencia de la ley aplicable a los hechos y actos relativos al estado civil.*

1. El contenido y vigencia del Derecho extranjero en relación con la adecuación a éste de un hecho o acto, la observancia de las formas y solemnidades extranjeras y la aptitud y capacidad legal necesarias para el acto, se podrán acreditar, entre otros medios, mediante la aseveración o informe de un Notario o Cónsul español, o de un Diplomático, Cónsul o autoridad competente del país cuya legislación resulte aplicable.

El Encargado del Registro podrá prescindir de dichos medios cuando conociere suficientemente la legislación extranjera de que se trate.

2. La falta de acreditación del contenido y vigencia del ordenamiento extranjero supondrá la denegación de la inscripción.

Disposición adicional primera. *Ubicación y dotación de las Oficinas del Registro Civil.*

1. Las Oficinas Generales del Registro Civil se ubicarán en las mismas localidades que correspondan a las sedes de los actuales Registros Civiles Municipales Principales, existentes a la entrada en vigor de esta Ley en las sedes de la capital de un partido judicial.

El Ministerio de Justicia, de oficio, previo informe de la Comunidad Autónoma afectada, o a iniciativa de la Comunidad Autónoma afectada, podrá modificar el número de Oficinas Generales del Registro Civil.

2. Los puestos de trabajo de las Oficinas del Registro Civil solo podrán ser cubiertos por personal de la Administración de Justicia, y se ordenarán de acuerdo con lo establecido en las correspondientes relaciones de puestos de trabajo.

3. Mediante el procedimiento previsto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para la ordenación e integración de las unidades que conforman las oficinas judiciales se determinarán las correspondientes relaciones de puestos de trabajo y las dotaciones del personal de la Administración de Justicia necesario para las Oficinas del Registro Civil. Las relaciones de puestos de trabajo podrán disponer la compatibilidad con funciones en oficina judicial en los casos en que así se prevea reglamentariamente.

Disposición adicional segunda. *Régimen jurídico de los Encargados del Registro Civil.*

1. En la forma y con los requisitos que reglamentariamente se determinen, las plazas de Encargados del Registro Civil se proveerán entre letrados de la Administración de Justicia. La convocatoria y resolución de los concursos para proveer las plazas corresponderá al Ministerio de Justicia. No obstante, las plazas de Encargados de la Oficina Central y de Encargados de aquellas Oficinas Generales que se ubiquen en las localidades donde se encontraban Registros Civiles Exclusivos se proveerán por el Ministerio de Justicia por el sistema de libre designación. El nombramiento y cese de las plazas provistas por el sistema de libre designación será a propuesta de las Comunidades Autónomas con competencias ejecutivas en Registro Civil o asumidas en materia de Justicia cuando dicha Oficina General esté situada en su ámbito territorial. El Encargado del Registro Civil recibirá la formación específica que determine el Ministerio de Justicia.

2. El ejercicio de esta función por los miembros del Cuerpo de letrados de la Administración de Justicia se considerará como situación de servicio activo en dicho Cuerpo y podrá ser compatible con funciones en oficina judicial en los casos en que así se prevea reglamentariamente y en la correspondiente Relación de Puestos de Trabajo.

3. El régimen de sustitución de los Encargados del Registro Civil se regulará reglamentariamente.

4. El incumplimiento o la inobservancia de las instrucciones, resoluciones y circulares de la Dirección General de Seguridad Jurídica y Fe Pública que derivasen de las facultades de supervisión e inspección de los registros civiles que corresponden a ese Centro Directivo o se pusieren de manifiesto por otra vía, se considerarán falta disciplinaria conforme a lo tipificado reglamentariamente.

Disposición adicional tercera. *Expedientes de nacionalidad por residencia.*

Las solicitudes de adquisición de nacionalidad española por residencia se iniciarán y tramitarán por los órganos de la Administración General del Estado que determine el Gobierno mediante Real Decreto.

Disposición adicional cuarta. *Constancia en el Registro Civil de los fallecimientos con posterioridad a los seis meses de gestación.*

Figurarán en un archivo del Registro Civil, sin efectos jurídicos, los fallecimientos que se produzcan con posterioridad a los seis meses de gestación y no cumplieran las condiciones previstas en el artículo 30 del Código Civil, pudiendo los progenitores otorgar un nombre.

Este archivo quedará sometido al régimen de publicidad restringida.

Disposición adicional quinta. *Oficinas colaboradoras del Registro Civil y punto de acceso en Ayuntamientos.*

Todas las secretarías de juzgados de paz o las unidades procesales de apoyo directo a juzgados de paz, o bien las oficinas de justicia en el municipio u otras del mismo tipo que se implanten en sustitución de las anteriores o como complemento de las mismas en virtud de ulteriores reformas legislativas, colaborarán con el Registro Civil desempeñando, en la forma que se desarrolle reglamentariamente, las funciones siguientes:

a) Recibirán por vía presencial y registrarán electrónicamente solicitudes, declaraciones o formularios, así como otros documentos necesarios para la tramitación de los procedimientos del Registro Civil.
b) Informarán a los ciudadanos en materias relacionadas con los procedimientos del Registro Civil.
c) Expedirán certificaciones de los asientos registrales obrantes en los libros físicos de Registro Civil que estén a su cargo y no puedan certificarse por medios electrónicos.
d) Expedirán certificaciones electrónicas de los asientos registrales, que se soliciten presencialmente en ellos.
e) Expedirán certificados de fe de vida.
f) Practicarán las actuaciones auxiliares no resolutivas que reglamentariamente se determinen.
g) Cualesquiera otras que determine la Dirección General de Seguridad Jurídica y Fe Pública.

En los municipios donde no se ubique una Oficina General, además de existir las Oficinas Colaboradoras con las funciones descritas anteriormente, los Ayuntamientos podrán solicitar al Ministerio de Justicia que les habilite las conexiones necesarias, conforme se regule reglamentariamente, para que los ciudadanos puedan presentar en dichos Ayuntamientos solicitudes y la documentación necesaria para las actuaciones ante el Registro Civil.

Las oficinas colaboradoras del Registro Civil no dispondrán de Encargado propio y para el desempeño de sus funciones se relacionarán con la Oficina General y el Encargado de su ámbito territorial. El Encargado de la Oficina General del ámbito territorial del que dependa una oficina colaboradora puede delegar funciones en el funcionario de los Cuerpos Generales de la Administración de Justicia de superior categoría que preste servicio en las oficinas colaboradoras o bien en el funcionario de la Administración local que sea expresamente designado por cada Ayuntamiento para atender dicha oficina de la localidad que no esté servida por funcionarios de la Administración de Justicia.

Disposición adicional sexta. *Uniformidad y dotación de los sistemas y aplicaciones informáticas en las Oficinas del Registro Civil.*

Todas las Oficinas del Registro Civil utilizarán los mismos sistemas y aplicaciones informáticas. El Ministerio de Justicia proveerá, tanto en su desarrollo como en su explotación, el conjunto de aplicaciones que soportan la actividad de los procesos operativos que se tramitan en el Registro Civil.

El Ministerio de Justicia y las Comunidades Autónomas con competencias ejecutivas en la materia o transferidas en medios materiales de Administración de Justicia, establecerán los mecanismos de coordinación necesarios para proporcionar los servicios de acceso a los sistemas del Registro Civil, soporte microinformático, formación y atención a usuarios.

Disposición adicional séptima. *Puesta a disposición de los datos de identificación personal de nacionales y extranjeros.*

Para la adecuada elaboración del código personal al que hace mención el artículo 6 de la presente Ley, así como para su uso en las aplicaciones informáticas en que sea preciso, el Ministerio del Interior pondrá a disposición del Ministerio de Justicia las respectivas secuencias alfanuméricas que atribuya el sistema informático vigente para el documento nacional de identidad y el número de identificación de extranjeros, así como los demás datos personales identificativos que consten en las bases de datos de ambos documentos.

De igual manera, el Ministerio de Justicia pondrá a disposición del Ministerio del Interior los datos personales identificativos inscritos en el Registro Civil que deban constar en el documento nacional de identidad o número de identificación de extranjeros.

Disposición adicional octava. *Inscripción de defunción de desaparecidos durante la guerra civil y la dictadura.*

El expediente registral, resuelto favorablemente, será título suficiente para practicar la inscripción de la defunción de las personas desaparecidas durante la Guerra Civil y la represión política inmediatamente posterior, siempre que, de las pruebas aportadas, pueda inferirse razonablemente su fallecimiento, aunque no sean inmediatas a éste. En la valoración de las pruebas se considerará especialmente el tiempo transcurrido, las circunstancias de peligro y la existencia de indicios de persecución o violencia.

Disposición adicional novena. *Obtención de datos del Instituto Nacional de Estadística.*

Para facilitar la tramitación telemática a los Registros Civiles, el Instituto Nacional de Estadística dará acceso telemático a los datos de domicilio relativos al Padrón municipal que guarden relación con los hechos inscribibles, así como, si fuera necesario para la correcta identificación de los citados hechos, a los datos de identificación que figuren en las inscripciones padronales, sin precisar para todo ello del consentimiento del interesado.

También se utilizarán los datos padronales para la actualización de la información obrante en las bases de datos de los Registros Civiles, en idénticas condiciones que en el párrafo anterior.

Disposición transitoria primera. *Procedimientos en tramitación a la entrada en vigor de la presente Ley.*

A los procedimientos y expedientes iniciados con anterioridad a la entrada en vigor de la presente Ley les será aplicable la Ley de 8 de junio de 1957, del Registro Civil, y las disposiciones dictadas en su desarrollo.

Disposición transitoria segunda. *Registros individuales.*

El Ministerio de Justicia adoptará las disposiciones necesarias para la progresiva incorporación de los datos digitalizados que consten en la base de datos del Registro Civil a registros individuales.

A tal efecto, se incorporarán a los registros individuales todas las inscripciones de nacimiento practicadas en los Registros Civiles municipales, tanto principales como delegados, Consulares y Central, desde 1920, y todas las inscripciones de matrimonio, defunciones y tutelas y demás representaciones legales practicadas en los Registros Civiles municipales, tanto principales como delegados, Consulares y Central, desde 1950.

El Ministerio de Justicia procederá a la recuperación informática de los asientos relativos a inscripciones anteriores a dichos años progresivamente, en función de las posibilidades presupuestarias.

Disposición transitoria tercera. *Libros de familia.*

A partir de la fecha de entrada en vigor de la presente Ley no se expedirán Libros de Familia.

Los Libros de Familia expedidos con anterioridad a la entrada en vigor de la presente Ley seguirán teniendo los efectos previstos en los artículos 8 y 75 de la Ley del Registro Civil de 8 de junio de 1957.

Disposición transitoria cuarta. *Extensión y práctica de asientos.*

Hasta que el Ministerio de Justicia apruebe, mediante resolución de la Dirección General de Seguridad Jurídica y Fe Pública, la entrada en servicio efectiva de las aplicaciones informáticas que permitan el funcionamiento del Registro Civil de forma íntegramente electrónica conforme a las previsiones contenidas en esta Ley, los Encargados de las Oficinas del Registro Civil practicarán en los libros y secciones correspondientes regulados

por la Ley de 8 de junio de 1957 los asientos relativos a nacimientos, matrimonios, defunciones, tutelas y representaciones legales. No resultará de aplicación, en tales casos, lo previsto en esta Ley respecto del código personal.

A dichos fines, mantendrán sus tareas y funciones de registro civil según lo previsto en el artículo 2.2 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en relación con los artículos 10 a 22 de la Ley del Registro Civil de 8 de junio de 1957, los que hasta el momento de la completa entrada en vigor de esta Ley hubiesen venido ejerciendo en los Registros Civiles como encargados, encargados por delegación, letrados de la Administración de Justicia y personal funcionario de los Cuerpos Generales de la Administración de Justicia y continuará aplicándose el artículo 27 de la Ley 38/1988, de 28 de diciembre, de Demarcación y de Planta Judicial.

Para la tramitación de procedimientos, expedición de publicidad y práctica de asientos en los términos del párrafo anterior, en tanto no se produzca la referida entrada en servicio de las aplicaciones informáticas, serán competentes las Oficinas del Registro Civil que lo vinieran siendo conforme a las reglas previstas en los artículos 15, 16, 17, 18 y 19 de la Ley del Registro Civil de 8 de junio de 1957, que seguirán aplicándose transitoriamente a estos solos efectos.

A fin de facilitar y agilizar la entrada en servicio efectivo de las aplicaciones informáticas, así como para agilizar la incorporación de datos digitalizados a los registros individuales, conforme a lo dispuesto en la disposición transitoria segunda de esta Ley, el Ministerio de Justicia, en colaboración con las Comunidades Autónomas con competencias en materia de Justicia, desarrollarán y presentarán proyectos adecuados en el marco del Plan de Transformación, Recuperación y Resiliencia.

El Gobierno, a través del Ministerio de Justicia, informará periódicamente a las Cortes Generales sobre el proceso de implantación del nuevo modelo de Registro Civil.

Disposición transitoria quinta. *Publicidad formal del Registro Civil no digitalizado.*

1. La publicidad formal de los datos incorporados a libros no digitalizados continuará rigiéndose por lo previsto en la Ley del Registro Civil de 8 de junio de 1957.

2. Se adecuarán los formatos y modelos de certificaciones al fin de posibilitar el uso de las lenguas oficiales.

Disposición transitoria sexta. *Valor histórico de los libros y documentos que obran en los archivos del Registro Civil.*

Los libros y documentos que a la fecha de la entrada en vigor de esta Ley obren en los archivos del Registro Civil se considerarán patrimonio documental con valor histórico en los términos previstos por la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, y por consiguiente no podrán ser destruidos.

Disposición transitoria séptima. *Oficinas Consulares de Registro Civil.*

Lo dispuesto en esta Ley se aplicará a las Oficinas Consulares de Registro Civil atendiendo a los medios y sistemas informáticos, los canales electrónicos y las condiciones de funcionamiento disponibles.

Disposición transitoria octava. *Creación de Oficinas del Registro Civil. Encargados y régimen transitorio de los letrados de la Administración de Justicia. Continuidad del personal al servicio de la Administración de Justicia destinado en el Registro Civil.*

1. A la entrada en servicio efectiva de las aplicaciones informáticas que permitan el funcionamiento del Registro Civil de forma íntegramente electrónica cuando así lo establezca la resolución o resoluciones que se dicten al amparo de la disposición transitoria cuarta, quedarán suprimidos los juzgados que, de forma exclusiva, hayan venido ejerciendo funciones de Registro Civil Exclusivo y de Registro Civil Central y, en su lugar, se crearán las Oficinas Generales de Registro Civil y la Oficina Central de Registro Civil.

En las demás poblaciones sedes de la capital de un partido judicial, a la entrada en servicio efectiva de las aplicaciones informáticas según lo indicado en el párrafo anterior, los Juzgados de Primera Instancia o de Primera Instancia e Instrucción que han venido

realizando las funciones de Registro Civil continuarán realizándolas, igualmente en calidad de Oficinas Generales de Registro Civil.

2. Los letrados de la Administración de Justicia que, en el momento de la entrada en servicio efectiva de las aplicaciones informáticas que permitan el funcionamiento del Registro Civil de forma íntegramente electrónica conforme a las previsiones contenidas en esta Ley, estén prestando servicios con destino definitivo en el Registro Civil Central o en los Registros Civiles Exclusivos allá donde los hubiere, así como los que tengan asignadas funciones de Registro Civil en los Juzgados de Primera Instancia o de Primera Instancia e Instrucción, pasarán a desempeñar las funciones de Encargados del Registro Civil, compatibilizándolas con las propias del cargo de letrado de la Administración de Justicia de la oficina judicial a la que hubiere estado adscrito el Registro Civil a la entrada en vigor de esta Ley. Las retribuciones serán las que se determinen en las relaciones de puestos de trabajo correspondientes, en atención a las funciones desarrolladas.

3. El personal funcionario al servicio de la Administración de Justicia que, en el momento de la entrada en servicio efectiva de las aplicaciones informáticas que permitan el funcionamiento del Registro Civil de forma íntegramente electrónica conforme a las previsiones contenidas en esta Ley, esté prestando servicios con destino definitivo en el Registro Civil Central y los Registros Civiles Exclusivos allá donde los hubiere o tenga asignadas funciones de registro en las oficinas judiciales con adscripción de Registro Civil, continuará desarrollando sus funciones respectivas de Registro Civil, compatibilizándolas, en su caso, con las que ejerza dentro de la Administración de Justicia en la oficina judicial a la que estuviera adscrito el Registro Civil, con abono de la totalidad de las retribuciones que viniese percibiendo.

4. En tanto no se implanten las estructuras y relaciones de puestos de trabajo oportunas en el ámbito del Registro Civil, se mantendrán los actuales centros de destino según lo previsto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Las nuevas Oficinas del Registro Civil que se implanten conforme a esta Ley se considerarán centro de destino para los funcionarios de la Administración de Justicia.

Las menciones que se realizan en el artículo 521 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, al Registro Civil han de entenderse hechas a las Oficinas Generales, Central y colaboradoras del Registro Civil que se establezcan en el territorio del Estado en virtud de lo previsto en esta Ley.

5. Tanto la elaboración de las relaciones de puestos de trabajo, como los procesos de acoplamiento del personal funcionario que se acometan para la creación de oficinas del Registro Civil, se regirán por las normas que sobre implantación de oficina judicial se contienen en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, así como en la normativa de desarrollo.

Disposición transitoria novena. *Aplicación de la disposición adicional cuarta.*

Lo dispuesto en la disposición adicional cuarta resultará de aplicación a todas aquellas defunciones acaecidas con anterioridad a su entrada en vigor, siempre que así lo soliciten los progenitores en el plazo de dos años desde su publicación en el «Boletín Oficial del Estado».

Disposición transitoria décima. *Destino de los Jueces Encargados de los Registros Civiles Exclusivos y de los Encargados del Registro Civil Central.*

1. Los jueces y magistrados que al momento de la entrada en servicio efectiva de las aplicaciones informáticas que permitan el funcionamiento del Registro Civil de forma íntegramente electrónica conforme a las previsiones de esta Ley, se encuentren prestando servicios con destino definitivo como Encargados de los Registros Civiles Exclusivos y del Registro Civil Central, podrán optar por mantenerse ejerciendo dichas funciones en situación de servicios especiales en la Carrera Judicial, siempre que hubieran accedido a dicha plaza antes del 22 de julio de 2011, fecha de publicación en el «Boletín Oficial del Estado» de esta Ley. Estas plazas se declararán a extinguir, pero mantendrán transitoriamente las mismas retribuciones que se estuvieran percibiendo antes de cambiar a la situación de servicios especiales y se amortizarán cuando cesen los titulares que las ocupasen. Aquellos jueces

que no desearan o no pudieran permanecer en esas funciones, quedarán en la situación que se prevé en los apartados finales de esta disposición.

2. Los asuntos jurisdiccionales pendientes de resolver se repartirán entre los juzgados de primera instancia o de primera instancia e instrucción según corresponda.

3. Las competencias jurisdiccionales atribuidas a jueces y magistrados por ostentar la condición de Encargados del Registro Civil, pasarán a corresponder a los juzgados de primera instancia o de primera instancia e instrucción conforme a las normas de competencia establecidas en las leyes procesales.

4. Los Jueces Encargados de los Registros Civiles exclusivos que con arreglo a lo dispuesto en esta Ley dejen de ostentar tal condición, quedarán provisionalmente a disposición del Presidente del Tribunal Superior de Justicia correspondiente, sin merma de las retribuciones que vinieren percibiendo. Mientras permanezcan en esta situación prestarán sus servicios en los puestos que determinen las respectivas Salas de Gobierno, devengando las indemnizaciones correspondientes por razón del servicio cuando éstos se prestaren en lugar distinto al del Registro Civil en el que estaban destinados, todo ello de conformidad con lo dispuesto en la Ley Orgánica del Poder Judicial. Estos Jueces serán destinados a los juzgados o tribunales del lugar y orden jurisdiccional de su elección, en la primera vacante que se produzca en el órgano elegido, a no ser que se trate de plazas de Presidente, de nombramiento discrecional o legalmente reservadas a magistrados procedentes de pruebas selectivas, salvo que éstos tuvieran esa condición, siempre y cuando reúnan el resto de condiciones objetivas previstas en la Ley Orgánica del Poder Judicial para poder acceder a dichas plazas.

5. Los Encargados de los Registros Civiles Centrales que por virtud de esta Ley dejen de ostentar tal condición quedarán adscritos a disposición del Presidente del Tribunal Superior de Justicia de Madrid. Mientras permanezcan en esta situación prestarán sus servicios en los puestos que determine la Sala de Gobierno y serán destinados a la primera vacante que se produzca en cualesquiera secciones civiles de la Audiencia Provincial de Madrid, a determinar por el Presidente, a no ser que se trate de las plazas de Presidente o legalmente reservadas a magistrados procedentes de pruebas selectivas, y para las que no se reconozca especial preferencia o reserva a especialista.

6. No obstante lo anterior, el tiempo durante el cual los jueces y magistrados afectados pueden permanecer en situación de adscripción provisional a las Presidencias de los Tribunales Superiores de Justicia podrá extenderse, a petición del propio interesado, a dos años a contar del momento en que perdieron la condición de Encargados del Registro Civil.

Disposición transitoria undécima. *Referencias a resoluciones judiciales en los expedientes en tramitación.*

Las menciones existentes en otras normas a autos y providencias que pudieran dictarse en los expedientes que se hallaren en tramitación en los Registros Civiles con arreglo a lo dispuesto en la Ley de 8 de junio de 1957, sobre el Registro Civil, y en el Decreto de 14 de noviembre de 1958, por el que se aprueba el Reglamento de la Ley del Registro Civil, se entenderán referidas a resoluciones del Encargado del Registro Civil.

Disposición derogatoria. *Ley de 8 de junio de 1957 del Registro Civil, Ley 38/1988, de 28 de diciembre, de Demarcación y de Planta Judicial, y Código Civil.*

Quedan derogadas cuantas normas se opongan a lo previsto en la presente Ley y, en particular, las siguientes:

1.ª Ley de 8 de junio de 1957, del Registro Civil, salvo en lo dispuesto en las disposiciones transitorias tercera, cuarta y quinta de esta Ley.

2.ª Los números 1 y 2 del artículo 27 de la Ley 38/1988, de 28 de diciembre, de Demarcación y de Planta Judicial, salvo en lo dispuesto en la disposición transitoria cuarta de esta Ley.

3.ª Los artículos 325 a 332 del Código Civil.

Disposición final primera. *Derecho supletorio.*

En todo lo no previsto en relación con la tramitación administrativa de los procedimientos regulados en la presente Ley se aplicará la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Disposición final segunda. *Referencias a los Encargados del Registro Civil y a los Alcaldes.*

1. Las referencias que se encuentren en cualquier norma referidas a Jueces o Magistrados encargados del Registro Civil se entenderán hechas al Encargado del Registro Civil, de conformidad con lo previsto en esta Ley.

2. Las referencias que se encuentren en cualquier norma al juez, alcalde o funcionario que haga sus veces competentes para autorizar el matrimonio civil, deben entenderse referidas al notario, Encargado del Registro Civil o funcionario diplomático o consular encargado del Registro Civil, para acreditar el cumplimiento de los requisitos de capacidad y la inexistencia de impedimentos o su dispensa; y al juez de paz, alcalde o concejal en quien éste delegue, Encargado del Registro Civil, notario, o funcionario diplomático o consular encargado del Registro Civil, para la celebración ante ellos del matrimonio en forma civil.

Disposición final tercera. *Reforma del Código Civil.*

Se modifica el artículo 30 del Código Civil, que queda redactado en los siguientes términos:

> **«Artículo 30.**
>
> La personalidad se adquiere en el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno.»

Disposición final cuarta. *Reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Se añade un nuevo párrafo 17.º al apartado 1 del artículo 52, se modifica la rúbrica del capítulo V del título I del libro IV y se añade un nuevo artículo 781 bis a la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en los siguientes términos:

Uno. Se añade un nuevo párrafo 17.º al apartado 1 del artículo 52 con la siguiente redacción:

> «17.º En los procesos contra las resoluciones y actos que dicte la Dirección General de los Registros y del Notariado en materia de Registro Civil, a excepción de las solicitudes de nacionalidad por residencia, será competente el Juzgado de Primera Instancia de la capital de provincia del domicilio del recurrente.»

Dos. Se modifica la rúbrica del capítulo V del título I del libro IV, que pasa a tener la siguiente redacción:

> «De la oposición a las resoluciones administrativas en materia de protección de menores, del procedimiento para determinar la necesidad de asentimiento en la adopción y de la oposición a determinadas resoluciones y actos de la Dirección General de los Registros y del Notariado en materia de Registro Civil.»

Tres. Se añade un nuevo artículo 781 bis con la siguiente redacción:

> **«Artículo 781 bis.** *Oposición a las resoluciones y actos de la Dirección General de los Registros y del Notariado en materia de Registro Civil.*
>
> 1. La oposición a las resoluciones de la Dirección General de los Registros y del Notariado en materia de Registro Civil, a excepción de las dictadas en materia de nacionalidad por residencia, podrá formularse en el plazo de dos meses desde su notificación, sin que sea necesaria la formulación de reclamación administrativa previa.

2. Quien pretenda oponerse a las resoluciones presentará un escrito inicial en el que sucintamente expresará su pretensión y la resolución a que se opone.

3. El secretario judicial reclamará a la Dirección General de los Registros y del Notariado un testimonio completo del expediente, que deberá ser aportado en el plazo de veinte días.

4. Recibido el testimonio del expediente administrativo, el secretario judicial emplazará al actor por veinte días para que presente la demanda, que se tramitará con arreglo a lo previsto en el artículo 753.»

Disposición final quinta. *Tasas municipales.*

Se añade un apartado 5 al artículo 20 del texto refundido de la Ley reguladora de las Haciendas Locales, aprobado por Real Decreto Legislativo 2/2004, de 5 de marzo, con la siguiente redacción:

«5. Los Ayuntamientos podrán establecer una tasa para la celebración de los matrimonios en forma civil.»

Disposición final quinta bis. *Aranceles notariales.*

El Gobierno aprobará los aranceles correspondientes a la intervención de los Notarios en la tramitación de las actas matrimoniales previas y por la celebración de matrimonios en forma civil con la autorización de las escrituras públicas correspondientes.

Disposición final sexta. *Adquisición de la nacionalidad española por los nietos de exiliados durante la guerra civil y la dictadura.*

El derecho de opción previsto en la disposición adicional séptima de la Ley 52/2007, de 26 de diciembre, por la que se reconocen y amplían derechos y se establecen medidas en favor de quienes padecieron persecución o violencia durante la guerra civil y la dictadura, podrán también ejercerlo los nietos de las exiliadas españolas que conservaron la nacionalidad española tras haber contraído matrimonio con un extranjero con posterioridad al 5 de agosto de 1954, fecha de entrada en vigor de la Ley de 15 julio de 1954, siempre que no transmitiesen la nacionalidad española a sus hijos, por seguir éstos la del padre, y formalicen su declaración en tal sentido en el plazo de un año desde la entrada en vigor de la presente disposición.

Disposición final séptima. *Competencias de las Comunidades Autónomas en materia de Registro Civil.*

Las Comunidades Autónomas tendrán participación en este ámbito ejerciendo las competencias ejecutivas en materia de Registro Civil o las que se deriven de competencias asumidas en materia de medios materiales y personales de la Administración de Justicia; de acuerdo con sus Estatutos de Autonomía, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y esta Ley, así como las demás disposiciones normativas.

Disposición final octava. *Título competencial.*

La presente Ley se dicta al amparo del artículo 149.1.5.ª y 8.ª de la Constitución Española, con excepción de la disposición final cuarta, que lo hace con base en el artículo 149.1.6.ª de la Constitución Española, que atribuye al Estado competencia exclusiva para dictar la legislación procesal.

Disposición final novena. *Desarrollo reglamentario.*

Se faculta al Gobierno para dictar cuantas disposiciones de aplicación y desarrollo de la presente Ley sean necesarias.

Disposición final décima. *Entrada en vigor.*

La presente Ley entrará en vigor el 30 de abril de 2021, excepto las disposiciones adicionales séptima y octava y las disposiciones finales tercera y sexta, que entrarán en

vigor al día siguiente de su publicación en el “Boletín Oficial del Estado”, y excepto los artículos 49.2 y 53 del mismo texto legal, que entrarán en vigor el día 30 de junio de 2017.

Lo dispuesto en el párrafo anterior se entiende sin perjuicio de la entrada en vigor el 15 de octubre de 2015 de los artículos 44, 45, 46, 47, 49.1 y 4, 64, 66 y 67.3, y la disposición adicional novena, en la redacción dada por el artículo 2 de la Ley 19/2015, de 13 de julio, de medidas de reforma administrativa en el ámbito de la Administración de Justicia y del Registro Civil.

Asimismo, esta Ley entrará en vigor para las oficinas consulares del Registro Civil el día 1 de octubre de 2020, aplicándose de forma progresiva de conformidad con lo previsto en la disposición transitoria séptima y las disposiciones reglamentarias que se dicten al efecto.

Hasta la completa entrada en vigor de esta Ley, el Gobierno adoptará las medidas y los cambios normativos necesarios que afecten a la organización y funcionamiento de los Registros Civiles.

§ 18

Ley 3/2007, de 15 de marzo, reguladora de la rectificación registral de la mención relativa al sexo de las personas

Jefatura del Estado
«BOE» núm. 65, de 16 de marzo de 2007
Última modificación: 12 de agosto de 2019
Referencia: BOE-A-2007-5585

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

EXPOSICIÓN DE MOTIVOS

La presente Ley tiene por objeto regular los requisitos necesarios para acceder al cambio de la inscripción relativa al sexo de una persona en el Registro Civil, cuando dicha inscripción no se corresponde con su verdadera identidad de género. Contempla también el cambio del nombre propio para que no resulte discordante con el sexo reclamado.

La transexualidad, considerada como un cambio de la identidad de género, ha sido ampliamente estudiada ya por la medicina y por la psicología. Se trata de una realidad social que requiere una respuesta del legislador, para que la inicial asignación registral del sexo y del nombre propio puedan ser modificadas, con la finalidad de garantizar el libre desarrollo de la personalidad y la dignidad de las personas cuya identidad de género no se corresponde con el sexo con el que inicialmente fueron inscritas.

De acuerdo con la regulación que se establece en esta Ley, la rectificación registral del sexo y el cambio del nombre se dirigen a constatar como un hecho cierto el cambio ya producido de la identidad de género, de manera que queden garantizadas la seguridad jurídica y las exigencias del interés general. Para ello, dicho cambio de identidad habrá de acreditarse debidamente, y la rectificación registral se llevará a cabo de acuerdo con la regulación de los expedientes gubernativos del Registro Civil.

Mediante esta Ley España se suma a aquellos países de nuestro entorno que cuentan con una legislación específica que da cobertura y seguridad jurídica a la necesidad de la persona transexual, adecuadamente diagnosticada, de ver corregida la inicial asignación registral de su sexo, asignación contradictoria con su identidad de género, así como a ostentar un nombre que no resulte discordante con su identidad.

Por último, se reforma mediante esta Ley el artículo 54 de la Ley del Registro Civil de 8 de junio de 1957. Para garantizar el derecho de las personas a la libre elección del nombre

propio, se deroga la prohibición de inscribir como nombre propio los diminutivos o variantes familiares y coloquiales que no hayan alcanzado sustantividad.

Artículo 1. *Legitimación.*

1. Toda persona de nacionalidad española, mayor de edad y con capacidad suficiente para ello, podrá solicitar la rectificación de la mención registral del sexo.

La rectificación del sexo conllevará el cambio del nombre propio de la persona, a efectos de que no resulte discordante con su sexo registral.

> Téngase en cuenta que se declara la inconstitucionalidad del apartado 1, pero únicamente en la medida que incluye en el ámbito subjetivo de la prohibición a los menores de edad con "suficiente madurez" y que se encuentren en una "situación estable de transexualidad", por Sentencia del TC 99/2019, de 18 de julio. Ref. BOE-A-2019-11911

2. Asimismo, la persona interesada podrá incluir en la solicitud la petición del traslado total del folio registral.

Artículo 2. *Procedimiento.*

1. La rectificación de la mención registral del sexo se tramitará y acordará con sujeción a las disposiciones de esta Ley, de acuerdo con las normas establecidas en la Ley del Registro Civil, de 8 de junio de 1957, para los expedientes gubernativos.

En la solicitud de rectificación registral se deberá incluir la elección de un nuevo nombre propio, salvo cuando la persona quiera conservar el que ostente y éste no sea contrario a los requisitos establecidos en la Ley del Registro Civil.

2. No son de aplicación en el expediente para la rectificación de la mención registral del sexo:

a) La regla primera del artículo 97 de la Ley del Registro Civil.

b) El párrafo segundo del artículo 218 del Reglamento del Registro Civil.

c) Los párrafos tercero y cuarto del artículo 349 del Reglamento del Registro Civil.

Artículo 3. *Autoridad competente.*

La competencia para conocer de las solicitudes de rectificación registral de la mención del sexo corresponderá al Encargado del Registro Civil del domicilio del solicitante.

Artículo 4. *Requisitos para acordar la rectificación.*

1. La rectificación registral de la mención del sexo se acordará una vez que la persona solicitante acredite:

a) Que le ha sido diagnosticada disforia de género.

La acreditación del cumplimiento de este requisito se realizará mediante informe de médico o psicólogo clínico, colegiados en España o cuyos títulos hayan sido reconocidos u homologados en España, y que deberá hacer referencia:

1. A la existencia de disonancia entre el sexo morfológico o género fisiológico inicialmente inscrito y la identidad de género sentida por el solicitante o sexo psicosocial, así como la estabilidad y persistencia de esta disonancia.

2. A la ausencia de trastornos de personalidad que pudieran influir, de forma determinante, en la existencia de la disonancia reseñada en el punto anterior.

b) Que ha sido tratada médicamente durante al menos dos años para acomodar sus características físicas a las correspondientes al sexo reclamado. La acreditación del cumplimiento de este requisito se efectuará mediante informe del médico colegiado bajo cuya dirección se haya realizado el tratamiento o, en su defecto, mediante informe de un médico forense especializado.

2. No será necesario para la concesión de la rectificación registral de la mención del sexo de una persona que el tratamiento médico haya incluido cirugía de reasignación sexual. Los tratamientos médicos a los que se refiere la letra b) del apartado anterior no serán un requisito necesario para la concesión de la rectificación registral cuando concurran razones de salud o edad que imposibiliten su seguimiento y se aporte certificación médica de tal circunstancia.

Artículo 5. *Efectos.*

1. La resolución que acuerde la rectificación de la mención registral del sexo tendrá efectos constitutivos a partir de su inscripción en el Registro Civil.
2. La rectificación registral permitirá a la persona ejercer todos los derechos inherentes a su nueva condición.
3. El cambio de sexo y nombre acordado no alterará la titularidad de los derechos y obligaciones jurídicas que pudieran corresponder a la persona con anterioridad a la inscripción del cambio registral.

Artículo 6. *Notificación del cambio registral de sexo.*

1. El Encargado del Registro Civil notificará de oficio el cambio de sexo y de nombre producido a las autoridades y organismos que reglamentariamente se determine.
2. El cambio de sexo y nombre obligará a quien lo hubiere obtenido a solicitar la emisión de un nuevo documento nacional de identidad ajustado a la inscripción registral rectificada. En todo caso se conservará el mismo número del documento nacional de identidad.
3. La nueva expedición de documentos con fecha anterior a la rectificación registral se realizará a petición del interesado, su representante legal o persona autorizada por aquel, debiendo garantizarse en todo caso por las autoridades, organismos e instituciones que los expidieron en su momento la adecuada identificación de la persona a cuyo favor se expidan los referidos documentos, mediante la oportuna impresión en el duplicado del documento del mismo número de documento nacional de identidad o la misma clave registral que figurare en el original.

Artículo 7. *Publicidad.*

No se dará publicidad sin autorización especial de la rectificación registral de la mención relativa al sexo de la persona.

Disposición adicional primera. *Adición de un apartado 3 al artículo 7 de la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida.*

Se modifica el artículo 7 de la Ley 14/2006, de 26 de mayo, sobre Técnicas de reproducción humana asistida, que queda redactado como sigue:

> **«Artículo 7.** *Filiación de los hijos nacidos mediante técnicas de reproducción asistida.*
>
> 1. La filiación de los nacidos con las técnicas de reproducción asistida se regulará por las leyes civiles, a salvo de las especificaciones establecidas en los tres siguientes artículos.
> 2. En ningún caso, la inscripción en el Registro Civil reflejará datos de los que se pueda inferir el carácter de la generación.
> 3. Cuando la mujer estuviere casada, y no separada legalmente o de hecho, con otra mujer, esta última podrá manifestar ante el Encargado del Registro Civil del domicilio conyugal, que consiente en que cuando nazca el hijo de su cónyuge, se determine a su favor la filiación respecto del nacido.»

Disposición adicional segunda. *Reexpedición de títulos o documentos.*

A efectos de abono de tasas por reexpedición de los títulos o documentos, la rectificación de la mención del sexo en el Registro Civil no se considera causa atribuible a la persona interesada.

Disposición transitoria única. *Exoneración de la acreditación de requisitos para la rectificación de la mención registral del sexo.*

La persona que, mediante informe de médico colegiado o certificado del médico del Registro Civil, acredite haber sido sometida a cirugía de reasignación sexual con anterioridad a la entrada en vigor de esta Ley, quedará exonerada de acreditar los requisitos previstos por el artículo 4.1.

Disposición final primera. *Título competencial.*

Esta Ley se dicta en ejercicio de las competencias exclusivas del Estado recogidas en el artículo 149.1. 8.ª de la Constitución.

Disposición final segunda. *Modificación de la Ley del Registro Civil, de 8 de junio de 1957.*

La Ley del Registro Civil, de 8 de junio de 1957, queda modificada como sigue:

Uno. El primer párrafo del artículo 6 quedará redactado de la siguiente forma:

> «El Registro es público para quienes tengan interés en conocer los asientos, con las excepciones que prevean ésta u otras leyes.»

Dos. El segundo párrafo del artículo 15 quedará redactado de la siguiente forma:

> «En todo caso se inscribirán los hechos ocurridos fuera de España, cuando las correspondientes inscripciones deban servir de base a inscripciones exigidas por el derecho español.»

Tres. El segundo párrafo del artículo 54 queda redactado como sigue:

> «Quedan prohibidos los nombres que objetivamente perjudiquen a la persona, los que hagan confusa la identificación y los que induzcan a error en cuanto al sexo.»

Cuatro. El artículo 93.2.º queda redactado como sigue:

> «2.º La indicación equivocada del sexo cuando igualmente no haya duda sobre la identidad del nacido por las demás circunstancias, así como la mención registral relativa al sexo de las personas en los casos de disforia de género.»

Disposición final tercera. *Desarrollo reglamentario.*

El Gobierno, a propuesta del Ministro de Justicia, dictará las disposiciones necesarias para el desarrollo y ejecución de esta Ley.

Disposición final cuarta. *Modificación de la Ley 84/1978, de 28 de diciembre, por la que se regula la tasa por expedición del Documento Nacional de Identidad.*

El número 2 del artículo 4 de la Ley 84/1978, de 28 de diciembre, queda redactado como sigue:

> «Quienes hubieran de renovar preceptivamente su documento durante el plazo de vigencia del mismo, por cambio de domicilio o de datos filiatorios, o por cualquier circunstancia no imputable al interesado.»

Disposición final quinta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 19

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 281, de 24 de noviembre de 1995
Última modificación: 2 de julio de 2021
Referencia: BOE-A-1995-25444

[. . .]

TÍTULO VII

De la extinción de la responsabilidad criminal y sus efectos

[. . .]

CAPÍTULO II

De la cancelación de antecedentes delictivos

Artículo 136.

1. Los condenados que hayan extinguido su responsabilidad penal tienen derecho a obtener del Ministerio de Justicia, de oficio o a instancia de parte, la cancelación de sus antecedentes penales, cuando hayan transcurrido sin haber vuelto a delinquir los siguientes plazos:

a) Seis meses para las penas leves.
b) Dos años para las penas que no excedan de doce meses y las impuestas por delitos imprudentes.
c) Tres años para las restantes penas menos graves inferiores a tres años.
d) Cinco años para las restantes penas menos graves iguales o superiores a tres años.
e) Diez años para las penas graves.

2. Los plazos a que se refiere el apartado anterior se contarán desde el día siguiente a aquel en que quedara extinguida la pena, pero si ello ocurriese mediante la remisión condicional, el plazo, una vez obtenida la remisión definitiva, se computará retrotrayéndolo al día siguiente a aquel en que hubiere quedado cumplida la pena si no se hubiere disfrutado de este beneficio. En este caso, se tomará como fecha inicial para el cómputo de la duración de la pena el día siguiente al del otorgamiento de la suspensión.

3. Las penas impuestas a las personas jurídicas y las consecuencias accesorias del artículo 129 se cancelarán en el plazo que corresponda, de acuerdo con la regla prevista en el apartado 1 de este artículo, salvo que se hubiese acordado la disolución o la prohibición

definitiva de actividades. En estos casos, se cancelarán las anotaciones transcurridos cincuenta años computados desde el día siguiente a la firmeza de la sentencia.

4. Las inscripciones de antecedentes penales en las distintas secciones del Registro Central de Penados y Rebeldes no serán públicas. Durante su vigencia solo se emitirán certificaciones con las limitaciones y garantías previstas en sus normas específicas y en los casos establecidos por la ley. En todo caso, se librarán las que soliciten los jueces o tribunales, se refieran o no a inscripciones canceladas, haciendo constar expresamente esta última circunstancia.

5. En los casos en que, a pesar de cumplirse los requisitos establecidos en este artículo para la cancelación, ésta no se haya producido, el juez o tribunal, acreditadas tales circunstancias, no tendrá en cuenta dichos antecedentes.

[. . .]

TÍTULO VI

Delitos contra la libertad

[. . .]

CAPÍTULO II

De las amenazas

Artículo 169.

El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:

1.º Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.

Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

2.º Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional.

Artículo 170.

1. Si las amenazas de un mal que constituyere delito fuesen dirigidas a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, o colectivo social o profesional, o a cualquier otro grupo de personas, y tuvieran la gravedad necesaria para conseguirlo, se impondrán respectivamente las penas superiores en grado a las previstas en el artículo anterior.

2. Serán castigados con la pena de prisión de seis meses a dos años, los que, con la misma finalidad y gravedad, reclamen públicamente la comisión de acciones violentas por parte de organizaciones o grupos terroristas.

Artículo 171.

1. Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior.

2. Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean

públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere.

3. Si el hecho descrito en el apartado anterior consistiere en la amenaza de revelar o denunciar la comisión de algún delito el ministerio fiscal podrá, para facilitar el castigo de la amenaza, abstenerse de acusar por el delito cuya revelación se hubiere amenazado, salvo que éste estuviere castigado con pena de prisión superior a dos años. En este último caso, el juez o tribunal podrá rebajar la sanción en uno o dos grados.

4. El que de modo leve amenace a quien sea o haya sido su esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, será castigado con la pena de prisión de seis meses a un año o de trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de un año y un día a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento hasta cinco años.

Igual pena se impondrá al que de modo leve amenace a una persona especialmente vulnerable que conviva con el autor.

5. El que de modo leve amenace con armas u otros instrumentos peligrosos a alguna de las personas a las que se refiere el artículo 173.2, exceptuadas las contempladas en el apartado anterior de este artículo, será castigado con la pena de prisión de tres meses a un año o trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de uno a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento por tiempo de seis meses a tres años.

Se impondrán las penas previstas en los apartados 4 y 5, en su mitad superior cuando el delito se perpetre en presencia de menores, o tenga lugar en el domicilio común o en el domicilio de la víctima, o se realice quebrantando una pena de las contempladas en el artículo 48 de este Código o una medida cautelar o de seguridad de la misma naturaleza.

6. No obstante lo previsto en los apartados 4 y 5, el Juez o Tribunal, razonándolo en sentencia, en atención a las circunstancias personales del autor y a las concurrentes en la realización del hecho, podrá imponer la pena inferior en grado.

7. Fuera de los casos anteriores, el que de modo leve amenace a otro será castigado con la pena de multa de uno a tres meses. Este hecho sólo será perseguible mediante denuncia de la persona agraviada o de su representante legal.

Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, la pena será la de localización permanente de cinco a treinta días, siempre en domicilio diferente y alejado del de la víctima, o trabajos en beneficio de la comunidad de cinco a treinta días, o multa de uno a cuatro meses, ésta última únicamente en los supuestos en los que concurran las circunstancias expresadas en el apartado 2 del artículo 84. En estos casos no será exigible la denuncia a que se refiere el párrafo anterior.

[. . .]

TÍTULO VII

De las torturas y otros delitos contra la integridad moral

Artículo 173.

1. El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

Con la misma pena serán castigados los que, en el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realicen contra otro de forma reiterada actos hostiles o humillantes que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima.

Se impondrá también la misma pena al que de forma reiterada lleve a cabo actos hostiles o humillantes que, sin llegar a constituir trato degradante, tengan por objeto impedir el legítimo disfrute de la vivienda.

2. El que habitualmente ejerza violencia física o psíquica sobre quien sea o haya sido su cónyuge o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, o sobre los descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente, o sobre los menores o personas con discapacidad necesitadas de especial protección que con él convivan o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente, o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de su convivencia familiar, así como sobre las personas que por su especial vulnerabilidad se encuentran sometidas a custodia o guarda en centros públicos o privados, será castigado con la pena de prisión de seis meses a tres años, privación del derecho a la tenencia y porte de armas de tres a cinco años y, en su caso, cuando el juez o tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento por tiempo de uno a cinco años, sin perjuicio de las penas que pudieran corresponder a los delitos en que se hubieran concretado los actos de violencia física o psíquica.

Se impondrán las penas en su mitad superior cuando alguno o algunos de los actos de violencia se perpetren en presencia de menores, o utilizando armas, o tengan lugar en el domicilio común o en el domicilio de la víctima, o se realicen quebrantando una pena de las contempladas en el artículo 48 o una medida cautelar o de seguridad o prohibición de la misma naturaleza.

En los supuestos a que se refiere este apartado, podrá además imponerse una medida de libertad vigilada.

3. Para apreciar la habitualidad a que se refiere el apartado anterior, se atenderá al número de actos de violencia que resulten acreditados, así como a la proximidad temporal de los mismos, con independencia de que dicha violencia se haya ejercido sobre la misma o diferentes víctimas de las comprendidas en este artículo, y de que los actos violentos hayan sido o no objeto de enjuiciamiento en procesos anteriores.

4. Quien cause injuria o vejación injusta de carácter leve, cuando el ofendido fuera una de las personas a las que se refiere el apartado 2 del artículo 173, será castigado con la pena de localización permanente de cinco a treinta días, siempre en domicilio diferente y alejado del de la víctima, o trabajos en beneficio de la comunidad de cinco a treinta días, o multa de uno a cuatro meses, esta última únicamente en los supuestos en los que concurran las circunstancias expresadas en el apartado 2 del artículo 84.

Las injurias solamente serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

[. . .]

TÍTULO VIII

Delitos contra la libertad e indemnidad sexuales

[. . .]

CAPÍTULO V

De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.

[. . .]

Artículo 189.

1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

a) Cuando se utilice a menores de dieciséis años.

b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio, se emplee violencia física o sexual para la obtención del material pornográfico o se representen escenas de violencia física o sexual.

c) Cuando se utilice a personas menores de edad que se hallen en una situación de especial vulnerabilidad por razón de enfermedad, discapacidad o por cualquier otra circunstancia.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

e) Cuando el material pornográfico fuera de notoria importancia.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, de la persona menor de edad o persona con discapacidad necesitada de especial protección, o se trate de cualquier persona que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.

h) Cuando concurra la agravante de reincidencia.

3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores.

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses.

7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español.

Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.

[. . .]

TÍTULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPÍTULO I

Del descubrimiento y revelación de secretos

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 197 quater.

Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

Artículo 197 quinquies.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 198.

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199.

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.
2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200.

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

Artículo 201.

1. Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal.
2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales, a una pluralidad de personas o si la víctima es una persona menor de edad o una persona con discapacidad necesitada de especial protección.
3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el artículo 130.1.5.º, párrafo segundo.

[. . .]

TÍTULO XI

Delitos contra el honor

CAPÍTULO I

De la calumnia

Artículo 205.

Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

[. . .]

CAPÍTULO II

De la injuria

Artículo 208.

Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves, sin perjuicio de lo dispuesto en el apartado 4 del artículo 173.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

[. . .]

CAPÍTULO III

Disposiciones generales

[. . .]

Artículo 216.

En los delitos de calumnia o injuria se considera que la reparación del daño comprende también la publicación o divulgación de la sentencia condenatoria, a costa del condenado por tales delitos, en el tiempo y forma que el Juez o Tribunal consideren más adecuado a tal fin, oídas las dos partes.

[. . .]

Sección 2.ª bis De la apropiación indebida

[. . .]

§ 20

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 157, de 2 de julio de 1985
Última modificación: 2 de julio de 2021
Referencia: BOE-A-1985-12666

[. . .]

LIBRO III

DEL RÉGIMEN DE LOS JUZGADOS Y TRIBUNALES

[. . .]

TÍTULO III

De las actuaciones judiciales

[. . .]

CAPÍTULO V

De la vista, votación y fallo

[. . .]

Artículo 266.

1. Las sentencias, una vez extendidas y firmadas por el juez o por todos los Magistrados que las hubieren dictado, serán depositadas en la Oficina judicial y se permitirá a cualquier interesado el acceso al texto de las mismas.

El acceso al texto de las sentencias, o a determinados extremos de las mismas, podrá quedar restringido cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes.

2. Los secretarios pondrán en los autos certificación literal de la sentencia.

[. . .]

Artículo 551.

1. La representación y defensa del Estado y de sus organismos autónomos, así como la representación y defensa de los órganos constitucionales cuyas normas internas no establezcan un régimen especial propio, corresponderá a los Abogados del Estado integrados en el Servicio Jurídico del Estado. Los Abogados del Estado podrán representar y defender a los restantes organismos y entidades públicos, sociedades mercantiles estatales y fundaciones con participación estatal, en los términos contenidos en la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica al Estado e Instituciones Públicas y disposiciones de desarrollo.

La representación y defensa de las entidades gestoras, servicios comunes y otros organismos o entidades de naturaleza pública, que conforme a la ley integran la Administración de la Seguridad Social, sin incluir, en consecuencia, la de las mutuas colaboradoras de la Seguridad Social, corresponderá a los Letrados de la Administración de la Seguridad Social, integrados en el Servicio Jurídico de la Administración de la Seguridad Social, sin perjuicio de que, de acuerdo con lo que reglamentariamente se determine, tales funciones puedan ser encomendadas a Abogado colegiado especialmente designado al efecto.

2. La representación y defensa de las Cortes Generales, del Congreso de los Diputados, del Senado, de la Junta Electoral Central y de los órganos e instituciones vinculados o dependientes de aquéllas corresponderá a los Letrados de las Cortes Generales integrados en las secretarías generales respectivas.

3. La representación y defensa de las comunidades autónomas y las de los entes locales corresponderán a los letrados que sirvan en los servicios jurídicos de dichas Administraciones públicas, salvo que designen abogado colegiado que les represente y defienda. Los Abogados del Estado podrán representar y defender a las comunidades autónomas y a los entes locales en los términos contenidos en la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica al Estado e Instituciones Públicas y su normativa de desarrollo.

[. . .]

LIBRO VIII

Del Consejo General del Poder Judicial

TÍTULO I

De las atribuciones del Consejo General del Poder Judicial

[. . .]

Artículo 560.

1. El Consejo General del Poder Judicial tiene las siguientes atribuciones:

1.ª Proponer el nombramiento, en los términos previstos por la presente Ley Orgánica, del Presidente del Tribunal Supremo y del Consejo General del Poder Judicial.

2.ª Proponer el nombramiento de Jueces, Magistrados y Magistrados del Tribunal Supremo.

3.ª Proponer el nombramiento, en los términos previstos por la presente Ley Orgánica, de dos Magistrados del Tribunal Constitucional.

4.ª Ser oído por el Gobierno antes del nombramiento del Fiscal General del Estado.

5.ª Interponer el conflicto de atribuciones entre órganos constitucionales del Estado, en los términos previstos por la Ley Orgánica del Tribunal Constitucional.

6.ª Participar, en los términos legalmente previstos, en la selección de Jueces y Magistrados.

7.ª Resolver lo que proceda en materia de formación y perfeccionamiento, provisión de destinos, ascensos, situaciones administrativas y régimen disciplinario de Jueces y Magistrados.

8.ª Ejercer la alta inspección de Tribunales, así como la supervisión y coordinación de la actividad inspectora ordinaria de los Presidentes y Salas de Gobierno de los Tribunales.

9.ª Impartir instrucciones a los órganos de gobierno de Juzgados y Tribunales en materias de la competencia de éstos, así como resolver los recursos de alzada que se interpongan contra cualesquiera acuerdos de los mismos.

10.ª Cuidar de la publicación oficial de las sentencias y demás resoluciones que se determinen del Tribunal Supremo y del resto de órganos judiciales.

A tal efecto el Consejo General del Poder Judicial, previo informe de las Administraciones competentes, establecerá reglamentariamente el modo en que se realizará la recopilación de las sentencias, su tratamiento, difusión y certificación, para velar por su integridad, autenticidad y acceso, así como para asegurar el cumplimiento de la legislación en materia de protección de datos personales.

11.ª Regular la estructura y funcionamiento de la Escuela Judicial, así como nombrar a su Director y a sus profesores.

12.ª Regular la estructura y funcionamiento del Centro de Documentación Judicial, así como nombrar a su Director y al resto de su personal.

13.ª Nombrar al Vicepresidente del Tribunal Supremo, al Promotor de la Acción Disciplinaria y al Jefe de la Inspección de Tribunales.

14.ª Nombrar al Director del Gabinete Técnico del Consejo General del Poder Judicial.

15.ª Regular y convocar el concurso-oposición de ingreso en el Cuerpo de Letrados del Consejo General del Poder Judicial.

16.ª Ejercer la potestad reglamentaria, en el marco estricto de desarrollo de las previsiones de la Ley Orgánica del Poder Judicial, en las siguientes materias:

a) Organización y funcionamiento del Consejo General del Poder Judicial.

b) Personal del Consejo General del Poder Judicial en el marco de la legislación sobre la función pública.

c) Órganos de gobierno de Juzgados y Tribunales.

d) Publicidad de las actuaciones judiciales.

e) Publicación y reutilización de las resoluciones judiciales.

f) Habilitación de días y horas, así como fijación de horas de audiencia pública.

g) Constitución de los órganos judiciales fuera de su sede.

h) Especialización de órganos judiciales.

i) Reparto de asuntos y ponencias.

j) Régimen de guardias de los órganos jurisdiccionales.

k) Organización y gestión de la actuación de los órganos judiciales españoles en materia de cooperación jurisdiccional interna e internacional.

l) **(Suprimida)**

m) Condiciones accesorias para el ejercicio de los derechos y deberes que conforman el estatuto de Jueces y Magistrados, así como el régimen jurídico de las Asociaciones judiciales, sin que tal desarrollo reglamentario pueda suponer innovación o alteración alguna de la regulación legal.

En ningún caso, las disposiciones reglamentarias del Consejo General del Poder Judicial podrán afectar o regular directa o indirectamente los derechos y deberes de personas ajenas al mismo.

17.ª Elaborar y ejecutar su propio presupuesto, en los términos previstos en la presente Ley Orgánica.

18.ª Aprobar la relación de puestos de trabajo del personal funcionario a su servicio.

19ª En materia de protección de datos personales, ejercerá las funciones definidas en el artículo 236 octies.

20.ª Recibir quejas de los ciudadanos en materias relacionadas con la Administración de Justicia.

21.ª Elaborar y aprobar, conjuntamente con el Ministerio de Justicia y, en su caso, oídas las Comunidades Autónomas cuando afectare a materias de su competencia, los sistemas

de racionalización, organización y medición de trabajo que se estimen convenientes para determinar la carga de trabajo que pueda soportar un órgano jurisdiccional.

La determinación de la carga de trabajo que cabe exigir, a efectos disciplinarios, al Juez o Magistrado corresponderá en exclusiva al Consejo General del Poder Judicial.

22.ª Proponer, previa justificación de la necesidad, las medidas de refuerzo que sean precisas en concretos órganos judiciales.

23.ª Emitir informe en los expedientes de responsabilidad patrimonial por anormal funcionamiento de la Administración de Justicia.

24.ª La recopilación y actualización de los Principios de Ética Judicial y su divulgación, así como su promoción con otras entidades y organizaciones judiciales, nacionales o internacionales.

El asesoramiento especializado a los jueces y magistrados en materia de conflictos de intereses, así como en las demás materias relacionadas con la integridad.

El Consejo General del Poder Judicial se asegurará de que la Comisión de Ética Judicial, que a tal efecto se constituya, esté dotada de los recursos y medios adecuados para el cumplimiento de sus objetivos.

25.ª Aquellas otras que le atribuya la Ley Orgánica del Poder Judicial.

2. Los proyectos de reglamentos de desarrollo se someterán a informe de las asociaciones profesionales de Jueces y Magistrados y de las corporaciones profesionales o asociaciones de otra naturaleza que tengan reconocida legalmente representación de intereses a los que puedan afectar. Se dará intervención a la Administración del Estado, por medio del Ministerio de Justicia, y a las de las Comunidades Autónomas siempre que una y otras tengan competencias relacionadas con el contenido del reglamento o sea necesario coordinar éstas con las del Consejo General. Se recabarán las consultas y los estudios previos que se consideren pertinentes y un dictamen de legalidad sobre el proyecto.

En todo caso, se elaborará un informe previo de impacto de género.

El Ministerio Fiscal será oído cuando le afecte la materia sobre la que verse el proyecto y especialmente en los supuestos contemplados en las letras d) y f) a j) del apartado 1.16.ª de este artículo.

3. **(Suprimido)**

4. Cuando en el ejercicio de las atribuciones legalmente previstas en este artículo el Consejo General del Poder Judicial adopte medidas que comporten un incremento de gasto, será preciso informe favorable de la Administración competente que deba soportar dicho gasto.

[. . .]

§ 21

Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional

Jefatura del Estado
«BOE» núm. 239, de 5 de octubre de 1979
Última modificación: 17 de octubre de 2015
Referencia: BOE-A-1979-23709

DON JUAN CARLOS I, REY DE ESPAÑA,

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado con el carácter de Orgánica y Yo vengo en sancionar la siguiente Ley:

TÍTULO I

Del Tribunal Constitucional

CAPÍTULO I

Del Tribunal Constitucional, su organización y atribuciones

Artículo primero.

Uno. El Tribunal Constitucional, como intérprete supremo de la Constitución, es independiente de los demás órganos constitucionales y está sometido sólo a la Constitución y a la presente Ley Orgánica.

Dos. Es único en su orden y extiende su jurisdicción a todo el territorio nacional.

Artículo segundo.

Uno. El Tribunal Constitucional conocerá en los casos y en la forma que esta Ley determina:

a) Del recurso y de la cuestión de inconstitucionalidad contra Leyes, disposiciones normativas o actos con fuerza de Ley.

b) Del recurso de amparo por violación de los derechos y libertades públicos relacionados en el artículo cincuenta y tres, dos, de la Constitución.

c) De los conflictos constitucionales de competencia entre el Estado y las Comunidades Autónomas o de los de éstas entre sí.

d) De los conflictos entre los órganos constitucionales del Estado.

d) bis. De los conflictos en defensa de la autonomía local.

e) De la declaración sobre la constitucionalidad de los tratados internacionales.

e) bis. Del control previo de inconstitucionalidad en el supuesto previsto en el artículo setenta y nueve de la presente Ley.

f) De las impugnaciones previstas en el número dos del artículo ciento sesenta y uno de la Constitución.

g) De la verificación de los nombramientos de los Magistrados del Tribunal Constitucional, para juzgar si los mismos reúnen los requisitos requeridos por la Constitución y la presente Ley.

h) De las demás materias que le atribuyen la Constitución y las Leyes orgánicas.

Dos. El Tribunal Constitucional podrá dictar reglamentos sobre su propio funcionamiento y organización, así como sobre el régimen de su personal y servicios, dentro del ámbito de la presente Ley. Estos reglamentos, que deberán ser aprobados por el Tribunal en Pleno, se publicarán en el «Boletín Oficial del Estado», autorizados por su Presidente.

Artículo tercero.

La competencia del Tribunal Constitucional se extiende al conocimiento y decisión de las cuestiones prejudiciales e incidentales no pertenecientes al orden constitucional, directamente relacionadas con la materia de que conoce, a los solos efectos del enjuiciamiento constitucional de ésta.

Artículo cuarto.

1. En ningún caso se podrá promover cuestión de jurisdicción o competencia al Tribunal Constitucional. El Tribunal Constitucional delimitará el ámbito de su jurisdicción y adoptará cuantas medidas sean necesarias para preservarla, incluyendo la declaración de nulidad de aquellos actos o resoluciones que la menoscaben; asimismo podrá apreciar de oficio o a instancia de parte su competencia o incompetencia.

2. Las resoluciones del Tribunal Constitucional no podrán ser enjuiciadas por ningún órgano jurisdiccional del Estado.

3. Cuando el Tribunal Constitucional anule un acto o resolución que contravenga lo dispuesto en los dos apartados anteriores lo ha de hacer motivadamente y previa audiencia al Ministerio Fiscal y al órgano autor del acto o resolución.

Artículo quinto.

El Tribunal Constitucional está integrado por doce miembros, con el título de Magistrados del Tribunal Constitucional.

Artículo sexto.

Uno. El Tribunal Constitucional actúa en Pleno, en Sala o en Sección.

Dos. El Pleno está integrado por todos los Magistrados del Tribunal. Lo preside el Presidente del Tribunal y, en su defecto, el Vicepresidente y, a falta de ambos, el Magistrado más antiguo en el cargo y, en caso de igual antigüedad, el de mayor edad.

Artículo séptimo.

Uno. El Tribunal Constitucional consta de dos Salas. Cada Sala está compuesta por seis Magistrados nombrados por el Tribunal en Pleno.

Dos. El Presidente del Tribunal lo es también de la Sala Primera, que presidirá en su defecto, el Magistrado más antiguo y, en caso de igual antigüedad, el de mayor edad.

Tres. El Vicepresidente del Tribunal presidirá en la Sala Segunda y, en su defecto, el Magistrado más antiguo y, en caso de igual antigüedad, el de mayor edad.

Artículo octavo.

1. Para el despacho ordinario y la decisión o propuesta, según proceda, sobre la admisibilidad o inadmisibilidad de procesos constitucionales, el Pleno y las Salas constituirán Secciones compuestas por el respectivo Presidente o quien le sustituya y dos Magistrados.

2. Se dará cuenta al Pleno de las propuestas de admisión o inadmisión de asuntos de su competencia. En el caso de admisión, el Pleno podrá deferir a la Sala que corresponda el conocimiento del asunto de que se trate, en los términos previstos en esta ley.

3. Podrá corresponder también a las Secciones el conocimiento y resolución de aquellos asuntos de amparo que la Sala correspondiente les defiera en los términos previstos en esta ley.

Artículo noveno.

Uno. El Tribunal en Pleno elige de entre sus miembros por votación secreta a su Presidente y propone al Rey su nombramiento.

Dos. En primera votación se requerirá la mayoría absoluta. Si ésta no se alcanzase se procederá a una segunda votación, en la que resultará elegido quien obtuviese mayor número de votos. En caso de empate se efectuará una última votación y si éste se repitiese, será propuesto el de mayor antigüedad en el cargo y en caso de igualdad el de mayor edad.

Tres. El nombre del elegido se elevará al Rey para su nombramiento por un período de tres años, expirado el cual podrá ser reelegido por una sola vez.

Cuatro. El Tribunal en Pleno elegirá entre sus miembros, por el procedimiento señalado en el apartado 2 de este artículo y por el mismo período de tres años, un Vicepresidente, al que incumbe sustituir al Presidente en caso de vacante, ausencia u otro motivo legal y presidir la Sala Segunda.

Artículo diez.

1. El Tribunal en Pleno conoce de los siguientes asuntos:

a) De la constitucionalidad o inconstitucionalidad de los tratados internacionales.

b) De los recursos de inconstitucionalidad contra las leyes y demás disposiciones con valor de ley, excepto los de mera aplicación de doctrina, cuyo conocimiento podrá atribuirse a las Salas en el trámite de admisión. Al atribuir a la Sala el conocimiento del recurso, el Pleno deberá señalar la doctrina constitucional de aplicación.

c) De las cuestiones de constitucionalidad que reserve para sí; las demás deberán deferirse a las Salas según un turno objetivo.

d) De los conflictos constitucionales de competencia entre el Estado y las Comunidades Autónomas o de los de éstas entre sí.

d) bis. De los recursos previos de inconstitucionalidad contra Proyectos de Estatutos de Autonomía y contra Propuestas de Reforma de los Estatutos de Autonomía.

e) De las impugnaciones previstas en el apartado 2 del artículo 161 de la Constitución.

f) De los conflictos en defensa de la autonomía local.

g) De los conflictos entre los órganos constitucionales del Estado.

h) De las anulaciones en defensa de la jurisdicción del Tribunal previstas en el artículo 4.3.

i) De la verificación del cumplimiento de los requisitos exigidos para el nombramiento de Magistrado del Tribunal Constitucional.

j) Del nombramiento de los Magistrados que han de integrar cada una de las Salas.

k) De la recusación de los Magistrados del Tribunal Constitucional.

l) Del cese de los Magistrados del Tribunal Constitucional en los casos previstos en el artículo 23.

m) De la aprobación y modificación de los reglamentos del Tribunal.

n) De cualquier otro asunto que sea competencia del Tribunal pero recabe para sí el Pleno, a propuesta del Presidente o de tres Magistrados, así como de los demás asuntos que le puedan ser atribuidos expresamente por una ley orgánica.

2. En los casos previstos en los párrafos d), e) y f) del apartado anterior, en el trámite de admisión la decisión de fondo podrá atribuirse a la Sala que corresponda según un turno objetivo, lo que se comunicará a las partes.

3. El Tribunal en Pleno, en ejercicio de su autonomía como órgano constitucional, elabora su presupuesto, que se integra como una sección independiente dentro de los Presupuestos Generales del Estado.

Artículo once.

Uno. Las Salas del Tribunal Constitucional conocerán de los asuntos que, atribuidos a la justicia constitucional, no sean de la competencia del Pleno.

Dos. También conocerán las Salas de aquellas cuestiones que, habiendo sido atribuidas al conocimiento de las Secciones, entiendan que por su importancia deba resolver la propia Sala.

Artículo doce.

La distribución de asuntos entre las Salas del Tribunal se efectuará según un turno establecido por el Pleno a propuesta de su Presidente.

Artículo trece.

Cuando una Sala considere necesario apartarse en cualquier punto de la doctrina constitucional precedente sentada por el Tribunal, la cuestión se someterá a la decisión del Pleno.

Artículo catorce.

El Tribunal en Pleno puede adoptar acuerdos cuando estén presentes, al menos, dos tercios de los miembros que en cada momento lo compongan. Los acuerdos de las Salas requerirán asimismo la presencia de dos tercios de los miembros que en cada momento las compongan. En las Secciones se requerirá la presencia de dos miembros, salvo que haya discrepancia, requiriéndose entonces la de sus tres miembros.

Artículo quince.

El Presidente del Tribunal Constitucional ejerce la representación del Tribunal, convoca y preside el Tribunal en Pleno y convoca las Salas; adopta las medidas precisas para el funcionamiento del Tribunal, de las Salas y de las Secciones; comunica a las Cámaras, al Gobierno o al Consejo General del Poder Judicial, en cada caso, las vacantes; nombra a los letrados, convoca los concursos para cubrir las plazas de funcionarios y los puestos de personal laboral, y ejerce las potestades administrativas sobre el personal del Tribunal.

CAPÍTULO II

De los Magistrados del Tribunal Constitucional

Artículo dieciséis.

Uno. Los Magistrados del Tribunal Constitucional serán nombrados por el Rey, a propuesta de las Cámaras, del Gobierno y del Consejo General del Poder Judicial, en las condiciones que establece el artículo ciento cincuenta y nueve, uno, de la Constitución.

Los Magistrados propuestos por el Senado serán elegidos entre los candidatos presentados por las Asambleas Legislativas de las Comunidades Autónomas en los términos que determine el Reglamento de la Cámara.

Dos. Los candidatos propuestos por el Congreso y por el Senado deberán comparecer previamente ante las correspondientes Comisiones en los términos que dispongan los respectivos Reglamentos.

Tres. La designación para el cargo de Magistrado del Tribunal Constitucional se hará por nueve años, renovándose el Tribunal por terceras partes cada tres. A partir de ese momento se producirá la elección del Presidente y Vicepresidente de acuerdo con lo previsto en el artículo 9. Si el mandato de tres años para el que fueron designados como Presidente y Vicepresidente no coincidiera con la renovación del Tribunal Constitucional, tal mandato quedará prorrogado para que finalice en el momento en que dicha renovación se produzca y tomen posesión los nuevos Magistrados.

Cuatro. Ningún Magistrado podrá ser propuesto al Rey para otro período inmediato, salvo que hubiera ocupado el cargo por un plazo no superior a tres años.

Cinco. Las vacantes producidas por causas distintas a la de la expiración del periodo para el que se hicieron los nombramientos serán cubiertas con arreglo al mismo procedimiento utilizado para la designación del Magistrado que hubiese causado vacante y por el tiempo que a éste restase. Si hubiese retraso en la renovación por tercios de los Magistrados, a los nuevos que fuesen designados se les restará del mandato el tiempo de retraso en la renovación.

Artículo diecisiete.

Uno. Antes de los cuatro meses previos a la fecha de expiración de los nombramientos, el Presidente del Tribunal solicitará de los Presidentes de los órganos que han de hacer las propuestas para la designación de los nuevos Magistrados, que inicien el procedimiento para ello.

Dos. Los Magistrados del Tribunal Constitucional continuarán en el ejercicio de sus funciones hasta que hayan tomado posesión quienes hubieren de sucederles.

Artículo dieciocho.

Los miembros del Tribunal Constitucional deberán ser nombrados entre ciudadanos españoles que sean Magistrados, Fiscales, Profesores de Universidad, funcionarios públicos o Abogados, todos ellos juristas de reconocida competencia con más de quince años de ejercicio profesional o en activo en la respectiva función.

Artículo diecinueve.

Uno. El cargo de Magistrado del Tribunal Constitucional es incompatible: Primero, con el de Defensor del Pueblo; segundo, con el de Diputado y Senador; tercero, con cualquier cargo político o administrativo del Estado, las Comunidades Autónomas, las provincias u otras Entidades locales; cuarto, con el ejercicio de cualquier jurisdicción o actividad propia de la carrera judicial o fiscal; quinto, con empleos de todas clases en los Tribunales y Juzgados de cualquier orden jurisdiccional; sexto, con el desempeño de funciones directivas en los partidos políticos, sindicatos, asociaciones, fundaciones y colegios profesionales y con toda clase de empleo al servicio de los mismos; séptimo, con el desempeño de actividades profesionales o mercantiles. En lo demás, los miembros del Tribunal Constitucional tendrán las incompatibilidades propias de los miembros del Poder Judicial.

Dos. Cuando concurriere causa de incompatibilidad en quien fuere propuesto como Magistrado del Tribunal, deberá, antes de tomar posesión, cesar en el cargo o en la actividad incompatible. Si no lo hiciere en el plazo de diez días siguientes a la propuesta, se entenderá que no acepta el cargo de Magistrado del Tribunal Constitucional. La misma regla se aplicará en el caso de incompatibilidad sobrevenida.

Artículo veinte.

Los miembros de la carrera judicial y fiscal y, en general, los funcionarios públicos nombrados Magistrados y letrados del Tribunal pasarán a la situación de servicios especiales en su carrera de origen.

Artículo veintiuno.

El Presidente y los demás Magistrados del Tribunal Constitucional prestarán, al asumir su cargo ante el Rey, el siguiente juramento o promesa:

«Juro (o prometo) guardar y hacer guardar fielmente y en todo tiempo la Constitución española, lealtad a la Corona y cumplir mis deberes como Magistrado Constitucional.»

Artículo veintidós.

Los Magistrados del Tribunal Constitucional ejercerán su función de acuerdo con los principios de imparcialidad y dignidad inherentes a la misma; no podrán ser perseguidos por las opiniones expresadas en el ejercicio de sus funciones; serán inamovibles y no podrán ser destituidos ni suspendidos sino por alguna de las causas que esta Ley establece.

Artículo veintitrés.

Uno. Los Magistrados del Tribunal Constitucional cesan por alguna de las causas siguientes: Primero, por renuncia aceptada por el Presidente del Tribunal; segundo, por expiración del plazo de su nombramiento; tercero, por incurrir en alguna causa de incapacidad de las previstas para los miembros del Poder Judicial; cuarto, por incompatibilidad sobrevenida; quinto, por dejar de atender con diligencia los deberes de su cargo; sexto, por violar la reserva propia de su función; séptimo, por haber sido declarado responsable civilmente por dolo o condenado por delito doloso o por culpa grave.

Dos. El cese o la vacante en el cargo de Magistrado del Tribunal Constitucional, en los casos primero y segundo, así como en el de fallecimiento, se decretará por el Presidente. En los restantes supuestos decidirá el Tribunal en Pleno, por mayoría simple en los casos tercero y cuarto y por mayoría de las tres cuartas partes de sus miembros en los demás casos.

Artículo veinticuatro.

Los Magistrados del Tribunal Constitucional podrán ser suspendidos por el Tribunal, como medida previa, en caso de procesamiento o por el tiempo indispensable para resolver sobre la concurrencia de alguna de las causas de cese establecidas en el artículo anterior. La suspensión requiere el voto favorable de las tres cuartas partes de los miembros del Tribunal reunido en Pleno.

Artículo veinticinco.

Uno. Los Magistrados del Tribunal que hubieran desempeñado el cargo durante un mínimo de tres años tendrán derecho a una remuneración de transición por un año, equivalente a la que percibieran en el momento del cese.

Dos. Cuando el Magistrado del Tribunal proceda de cualquier Cuerpo de funcionarios con derecho a jubilación, se le computará, a los efectos de determinación del haber pasivo, el tiempo de desempeño de las funciones constitucionales y se calculará aquél sobre el total de las remuneraciones que hayan correspondido al Magistrado del Tribunal Constitucional durante el último año.

Artículo veintiséis.

La responsabilidad criminal de los Magistrados del Tribunal Constitucional sólo será exigible ante la Sala de lo Penal del Tribunal Supremo.

TÍTULO II

De los procedimientos de declaración de inconstitucionalidad

CAPÍTULO I

Disposiciones generales

Artículo veintisiete.

Uno. Mediante los procedimientos de declaración de inconstitucionalidad regulados en este título, el Tribunal Constitucional garantiza la primacía de la Constitución y enjuicia la conformidad o disconformidad con ella de las Leyes, disposiciones o actos impugnados.

Dos. Son susceptibles de declaración de inconstitucionalidad:

a) Los Estatutos de Autonomía y las demás Leyes orgánicas.

b) Las demás Leyes, disposiciones normativas y actos del Estado con fuerza de Ley. En el caso de los Decretos legislativos, la competencia del Tribunal se entiende sin perjuicio de lo previsto en el número seis del artículo ochenta y dos de la Constitución.

c) Los Tratados Internacionales.

d) Los Reglamentos de las Cámaras y de las Cortes Generales.

e) Las Leyes, actos y disposiciones normativas con fuerza de Ley de las Comunidades Autónomas, con la misma salvedad formula en el apartado b) respecto a los casos de delegación legislativa.

f) Los Reglamentos de las Asambleas legislativas de las Comunidades Autónomas.

Artículo veintiocho.

Uno. Para apreciar la conformidad o disconformidad con la Constitución de una Ley, disposición o acto con fuerza de Ley del Estado o de las Comunidades Autónomas, el Tribunal considerará, además de los preceptos constitucionales, las Leyes que, dentro del marco constitucional, se hubieran dictado para delimitar las competencias del Estado y las diferentes Comunidades Autónomas o para regular o armonizar el ejercicio de las competencias de éstas.

Dos. Asimismo el Tribunal podrá declarar inconstitucionales por infracción del artículo ochenta y uno de la Constitución los preceptos de un Decreto-ley, Decreto legislativo, Ley que no haya sido aprobada con el carácter de orgánica o norma legislativa de una Comunidad Autónoma en el caso de que dichas disposiciones hubieran regulado materias reservadas a Ley Orgánica o impliquen modificación o derogación de una Ley aprobada con tal carácter, cualquiera que sea su contenido.

Artículo veintinueve.

Uno. La declaración de inconstitucionalidad podrá promoverse mediante:

a) El recurso de inconstitucionalidad.

b) La cuestión de inconstitucionalidad promovida por Jueces o Tribunales.

Dos. La desestimación, por razones de forma, de un recurso de inconstitucionalidad contra una Ley, disposición o acto con fuerza de Ley no será obstáculo para que la misma Ley, disposición o acto puedan ser objeto de una cuestión de inconstitucionalidad con ocasión de su aplicación en otro proceso.

Artículo treinta.

La admisión de un recurso o de una cuestión de inconstitucionalidad no suspenderá la vigencia ni la aplicación de la Ley, de la disposición normativa o del acto con fuerza de Ley, excepto en el caso en que el Gobierno se ampare en lo dispuesto por el artículo ciento sesenta y uno, dos, de la Constitución para impugnar, por medio de su Presidente, Leyes, disposiciones normativas o actos con fuerza de Ley de las Comunidades Autónomas.

CAPÍTULO II

Del recurso de inconstitucionalidad

Artículo treinta y uno.

El recurso de inconstitucionalidad contra las Leyes, disposiciones normativas o actos con fuerza de Ley podrá promoverse a partir de su publicación oficial.

Artículo treinta y dos.

Uno. Están legitimados para el ejercicio del recurso de inconstitucionalidad cuando se trate de Estatutos de Autonomía y demás Leyes del Estado, orgánicas o en cualesquiera de sus formas, y disposiciones normativas y actos del Estado o de las Comunidades Autónomas con fuerza de ley, Tratados Internacionales y Reglamentos de las Cámaras y de las Cortes Generales:

a) El Presidente del Gobierno.

b) El Defensor del Pueblo.

c) Cincuenta Diputados.

d) Cincuenta Senadores.

Dos. Para el ejercicio del recurso de inconstitucionalidad contra las Leyes, disposiciones o actos con fuerza de Ley del Estado que puedan afectar a su propio ámbito de autonomía, están también legitimados los órganos colegiados ejecutivos y las Asambleas de las Comunidades Autónomas, previo acuerdo adoptado al efecto.

Artículo treinta y tres.

1. El recurso de inconstitucionalidad se formulará dentro del plazo de tres meses a partir de la publicación de la Ley, disposición o acto con fuerza de Ley impugnado mediante demanda presentada ante el Tribunal Constitucional, en la que deberán expresarse las circunstancias de identidad de las personas u órganos que ejercitan la acción y, en su caso, de sus comisionados, concretar la Ley, disposición o acto impugnado, en todo o en parte, y precisar el precepto constitucional que se entiende infringido.

2. No obstante lo dispuesto en el apartado anterior, el Presidente del Gobierno y los órganos colegiados ejecutivos de las Comunidades Autónomas podrán interponer el recurso de inconstitucionalidad en el plazo de nueve meses contra leyes, disposiciones o actos con fuerza de Ley en relación con las cuales, y con la finalidad de evitar la interposición del recurso, se cumplan los siguientes requisitos:

a) Que se reúna la Comisión Bilateral de Cooperación entre la Administración General del Estado y la respectiva Comunidad Autónoma, pudiendo solicitar su convocatoria cualquiera de las dos Administraciones.

b) Que en el seno de la mencionada Comisión Bilateral se haya adoptado un acuerdo sobre iniciación de negociaciones para resolver las discrepancias, pudiendo instar, en su caso, la modificación del texto normativo. Este acuerdo podrá hacer referencia a la invocación o no de la suspensión de la norma en el caso de presentarse el recurso en el plazo previsto en este apartado.

c) Que el acuerdo sea puesto en conocimiento del Tribunal Constitucional por los órganos anteriormente mencionados dentro de los tres meses siguientes a la publicación de la Ley, disposición o acto con fuerza de Ley, y se inserte en el "Boletín Oficial del Estado" y en el "Diario Oficial" de la Comunidad Autónoma correspondiente.

3. Lo señalado en el apartado anterior se entiende sin perjuicio de la facultad de interposición del recurso de inconstitucionalidad por los demás órganos y personas a que hace referencia el artículo 32.

Artículo treinta y cuatro.

Uno. Admitida a trámite la demanda, el Tribunal Constitucional dará traslado de la misma al Congreso de los Diputados y al Senado por conducto de sus Presidentes, al Gobierno por conducto del Ministerio de Justicia y, en caso de que el objeto del recurso fuera una Ley o disposición con fuerza de Ley dictada por una Comunidad Autónoma, a los órganos legislativo y ejecutivo de la misma a fin de que puedan personarse en el procedimiento y formular las alegaciones que estimaren oportunas.

Dos. La personación y la formulación de alegaciones deberán hacerse en el plazo de quince días, transcurrido el cual el Tribunal dictará sentencia en el de diez, salvo que, mediante resolución motivada, el propio Tribunal estime necesario un plazo más amplio que, en ningún caso, podrá exceder de treinta días.

CAPÍTULO III

De la cuestión de inconstitucionalidad promovida por Jueces o Tribunales

Artículo treinta y cinco.

Uno. Cuando un Juez o Tribunal, de oficio o a instancia de parte, considere que una norma con rango de Ley aplicable al caso y de cuya validez dependa el fallo pueda ser contraria a la Constitución, planteará la cuestión al Tribunal Constitucional con sujeción a lo dispuesto en esta Ley.

Dos. El órgano judicial sólo podrá plantear la cuestión una vez concluso el procedimiento y dentro del plazo para dictar sentencia, o la resolución jurisdiccional que procediese, y deberá concretar la ley o norma con fuerza de ley cuya constitucionalidad se cuestiona, el precepto constitucional que se supone infringido y especificar o justificar en qué medida la decisión del proceso depende de la validez de la norma en cuestión. Antes de adoptar mediante auto su decisión definitiva, el órgano judicial oirá a las partes y al Ministerio Fiscal para que en el plazo común e improrrogable de 10 días puedan alegar lo que deseen sobre la pertinencia de plantear la cuestión de inconstitucionalidad, o sobre el fondo de ésta; seguidamente y sin más trámite, el juez resolverá en el plazo de tres días. Dicho auto no será susceptible de recurso de ninguna clase. No obstante, la cuestión de inconstitucionalidad podrá ser intentada de nuevo en las sucesivas instancias o grados en tanto no se llegue a sentencia firme.

Tres. El planteamiento de la cuestión de constitucionalidad originará la suspensión provisional de las actuaciones en el proceso judicial hasta que el Tribunal Constitucional se pronuncie sobre su admisión. Producida ésta el proceso judicial permanecerá suspendido hasta que el Tribunal Constitucional resuelva definitivamente sobre la cuestión.

Artículo treinta y seis.

El órgano judicial elevará al Tribunal Constitucional la cuestión de inconstitucionalidad junto con testimonio de los autos principales y de las alegaciones previstas en el artículo anterior, si las hubiere.

Artículo treinta y siete.

Uno. Recibidas en el Tribunal Constitucional las actuaciones, el procedimiento se sustanciará por los trámites del apartado segundo de este artículo. No obstante, podrá el Tribunal rechazar, en trámite de admisión, mediante auto y sin otra audiencia que la del Fiscal General del Estado, la cuestión de inconstitucionalidad cuando faltaren las condiciones procesales o fuere notoriamente infundada la cuestión suscitada. Esta decisión será motivada.

Dos. Publicada en el "Boletín Oficial del Estado" la admisión a trámite de la cuestión de inconstitucionalidad, quienes sean parte en el procedimiento judicial podrán personarse ante el Tribunal Constitucional dentro de los 15 días siguientes a su publicación, para formular alegaciones, en el plazo de otros 15 días.

Tres. El Tribunal Constitucional dará traslado de la cuestión al Congreso de los Diputados y al Senado por conducto de sus Presidentes, al Fiscal General del Estado, al Gobierno, por conducto del Ministerio de Justicia, y, en caso de afectar a una Ley o a otra disposición normativa con fuerza de Ley dictadas por una Comunidad Autónoma, a los órganos legislativo y ejecutivo de la misma, todos los cuales podrán personarse y formular alegaciones sobre la cuestión planteada en el plazo común improrrogable de quince días. Concluido éste, el Tribunal dictará sentencia en el plazo de quince días, salvo que estime necesario, mediante resolución motivada, un plazo más amplio, que no podrá exceder de treinta días.

CAPÍTULO IV

De la sentencia en procedimientos de inconstitucionalidad y de sus efectos

Artículo treinta y ocho.

Uno. Las sentencias recaídas en procedimientos de inconstitucionalidad tendrán el valor de cosa juzgada, vincularán a todos los Poderes Públicos y producirán efectos generales desde la fecha de su publicación en el «Boletín Oficial del Estado».

Dos. Las sentencias desestimatorias dictadas en recursos de inconstitucionalidad y en conflictos en defensa de la autonomía local impedirán cualquier planteamiento ulterior de la cuestión por cualquiera de las dos vías, fundado en la misma infracción de idéntico precepto constitucional.

Tres. Si se tratare de sentencias recaídas en cuestiones de inconstitucionalidad, el Tribunal Constitucional lo comunicará inmediatamente al órgano judicial competente para la decisión del proceso. Dicho órgano notificará la sentencia constitucional a las partes. El Juez o Tribunal quedará vinculado desde que tuviere conocimiento de la sentencia constitucional y las partes desde el momento en que sean notificadas.

Artículo treinta y nueve.

Uno. Cuando la sentencia declare la inconstitucionalidad, declarará igualmente la nulidad de los preceptos impugnados, así como, en su caso, la de aquellos otros de la misma Ley, disposición o acto con fuerza de Ley a los que deba extenderse por conexión o consecuencia.

Dos. El Tribunal Constitucional podrá fundar la declaración de inconstitucionalidad en la infracción de cualquier precepto constitucional, haya o no sido invocado en el curso del proceso.

Artículo cuarenta.

Uno. Las sentencias declaratorias de la inconstitucionalidad de Leyes, disposiciones o actos con fuerza de Ley no permitirán revisar procesos fenecidos mediante sentencia con fuerza de cosa juzgada en los que se haya hecho aplicación de las Leyes, disposiciones o actos inconstitucionales, salvo en el caso de los procesos penales o contencioso-administrativos referentes a un procedimiento sancionador en que, como consecuencia de la nulidad de la norma aplicada, resulte una reducción de la pena o de la sanción o una exclusión, exención o limitación de la responsabilidad.

Dos. En todo caso, la jurisprudencia de los tribunales de justicia recaída sobre leyes, disposiciones o actos enjuiciados por el Tribunal Constitucional habrá de entenderse corregida por la doctrina derivada de las sentencias y autos que resuelvan los procesos constitucionales.

TÍTULO III

Del recurso de amparo constitucional

CAPÍTULO I

De la procedencia e interposición del recurso de amparo constitucional

Artículo cuarenta y uno.

Uno. Los derechos y libertades reconocidos en los artículos catorce a veintinueve de la Constitución serán susceptibles de amparo constitucional, en los casos y formas que esta Ley establece, sin perjuicio de su tutela general encomendada a los Tribunales de Justicia. Igual protección será aplicable a la objeción de conciencia reconocida en el artículo treinta de la Constitución.

Dos. El recurso de amparo constitucional protege, en los términos que esta ley establece, frente a las violaciones de los derechos y libertades a que se refiere el apartado anterior, originadas por las disposiciones, actos jurídicos, omisiones o simple vía de hecho de los poderes públicos del Estado, las Comunidades Autónomas y demás entes públicos de carácter territorial, corporativo o institucional, así como de sus funcionarios o agentes.

Tres. En el amparo constitucional no pueden hacerse valer otras pretensiones que las dirigidas a restablecer o preservar los derechos o libertades por razón de los cuales se formuló el recurso.

Artículo cuarenta y dos.

Las decisiones o actos sin valor de Ley, emanados de las Cortes o de cualquiera de sus órganos, o de las Asambleas legislativas de las Comunidades Autónomas, o de sus órganos, que violen los derechos y libertades susceptibles de amparo constitucional, podrán ser

recurridos dentro del plazo de tres meses desde que, con arreglo a las normas internas de las Cámaras o Asambleas, sean firmes.

Artículo cuarenta y tres.

Uno. Las violaciones de los derechos y libertades antes referidos originadas por disposiciones, actos jurídicos, omisiones o simple vía de hecho del Gobierno o de sus autoridades o funcionarios, o de los órganos ejecutivos colegiados de las comunidades autónomas o de sus autoridades o funcionarios o agentes, podrán dar lugar al recurso de amparo una vez que se haya agotado la vía judicial procedente.

Dos. El plazo para interponer el recurso de amparo constitucional será el de los veinte días siguientes a la notificación de la resolución recaída en el previo proceso judicial.

Tres. El recurso sólo podrá fundarse en la infracción por una resolución firme de los preceptos constitucionales que reconocen los derechos o libertades susceptibles de amparo.

Artículo cuarenta y cuatro.

1. Las violaciones de los derechos y libertades susceptibles de amparo constitucional, que tuvieran su origen inmediato y directo en un acto u omisión de un órgano judicial, podrán dar lugar a este recurso siempre que se cumplan los requisitos siguientes:

a) Que se hayan agotado todos los medios de impugnación previstos por las normas procesales para el caso concreto dentro de la vía judicial.

b) Que la violación del derecho o libertad sea imputable de modo inmediato y directo a una acción u omisión del órgano judicial con independencia de los hechos que dieron lugar al proceso en que aquellas se produjeron, acerca de los que, en ningún caso, entrará a conocer el Tribunal Constitucional.

c) Que se haya denunciado formalmente en el proceso, si hubo oportunidad, la vulneración del derecho constitucional tan pronto como, una vez conocida, hubiera lugar para ello.

2. El plazo para interponer el recurso de amparo será de 30 días, a partir de la notificación de la resolución recaída en el proceso judicial.

Artículo cuarenta y cinco.

(Derogado)

Artículo cuarenta y seis.

Uno. Están legitimados para interponer el recurso de amparo constitucional:

a) En los casos de los artículos cuarenta y dos y cuarenta y cinco, la persona directamente afectada, el Defensor del Pueblo y el Ministerio Fiscal.

b) En los casos de los artículos cuarenta y tres y cuarenta y cuatro, quienes hayan sido parte en el proceso judicial correspondiente, el Defensor del Pueblo y el Ministerio Fiscal.

Dos. Si el recurso se promueve por el Defensor del Pueblo o el Ministerio Fiscal, la Sala competente para conocer del amparo constitucional lo comunicara a los posibles agraviados que fueran conocidos y ordenará anunciar la interposición del recurso en el «Boletín Oficial del Estado» a efectos de comparecencia de otros posibles interesados. Dicha publicación tendrá carácter preferente.

Artículo cuarenta y siete.

Uno. Podrán comparecer en el proceso de amparo constitucional, con el carácter de demandado o con el de coadyuvante, las personas favorecidas por la decisión, acto o hecho en razón del cual se formule el recurso que ostenten un interés legítimo en el mismo.

Dos. El Ministerio Fiscal intervendrá en todos los procesos de amparo, en defensa de la legalidad, de los derechos de los ciudadanos y del interés público tutelado por la Ley.

CAPÍTULO II

De la tramitación de los recursos de amparo constitucional

Artículo cuarenta y ocho.

El conocimiento de los recursos de amparo constitucional corresponde a las Salas del Tribunal Constitucional y, en su caso, a las Secciones.

Artículo cuarenta y nueve.

Uno. El recurso de amparo constitucional se iniciará mediante demanda en la que se expondrán con claridad y concisión los hechos que la fundamenten, se citarán los preceptos constitucionales que se estimen infringidos y se fijará con precisión el amparo que se solicita para preservar o restablecer el derecho o libertad que se considere vulnerado. En todo caso, la demanda justificará la especial trascendencia constitucional del recurso.

Dos. Con la demanda se acompañarán:

a) El documento que acredite la representación del solicitante del amparo.

b) En su caso, la copia, traslado o certificación de la resolución recaída en el procedimiento judicial o administrativo.

Tres. A la demanda se acompañarán también tantas copias literales de la misma y de los documentos presentados como partes en el previo proceso, si lo hubiere, y una más para el Ministerio Fiscal.

Cuatro. De incumplirse cualquiera de los requisitos establecidos en los apartados que anteceden, las Secretarías de Justicia lo pondrán de manifiesto al interesado en el plazo de 10 días, con el apercibimiento de que, de no subsanarse el defecto, se acordará la inadmisión del recurso.

Artículo cincuenta.

1. El recurso de amparo debe ser objeto de una decisión de admisión a trámite. La Sección, por unanimidad de sus miembros, acordará mediante providencia la admisión, en todo o en parte, del recurso solamente cuando concurran todos los siguientes requisitos:

a) Que la demanda cumpla con lo dispuesto en los artículos 41 a 46 y 49.

b) Que el contenido del recurso justifique una decisión sobre el fondo por parte del Tribunal Constitucional en razón de su especial trascendencia constitucional, que se apreciará atendiendo a su importancia para la interpretación de la Constitución, para su aplicación o para su general eficacia, y para la determinación del contenido y alcance de los derechos fundamentales.

2. Cuando la admisión a trámite, aun habiendo obtenido la mayoría, no alcance la unanimidad, la Sección trasladará la decisión a la Sala respectiva para su resolución.

3. Las providencias de inadmisión, adoptadas por las Secciones o las Salas, especificarán el requisito incumplido y se notificarán al demandante y al Ministerio Fiscal. Dichas providencias solamente podrán ser recurridas en súplica por el Ministerio Fiscal en el plazo de tres días. Este recurso se resolverá mediante auto, que no será susceptible de impugnación alguna.

4. Cuando en la demanda de amparo concurran uno o varios defectos de naturaleza subsanable, se procederá en la forma prevista en el artículo 49.4; de no producirse la subsanación dentro del plazo fijado en dicho precepto, la Sección acordará la inadmisión mediante providencia, contra la cual no cabrá recurso alguno

Artículo cincuenta y uno.

Uno. Admitida la demanda de amparo, la Sala requerirá con carácter urgente al órgano o a la autoridad de que dimane la decisión, el acto o el hecho, o al Juez o Tribunal que conoció del procedimiento precedente para que, en plazo que no podrá exceder de diez días, remita las actuaciones o testimonio de ellas.

Dos. El órgano, autoridad, Juez o Tribunal acusará inmediato recibo del requerimiento, cumplimentará el envío dentro del plazo señalado y emplazará a quienes fueron parte en el procedimiento antecedente para que puedan comparecer en el proceso constitucional en el plazo de diez días.

Artículo cincuenta y dos.

Uno. Recibidas las actuaciones y transcurrido el tiempo de emplazamiento, la Sala dará vista de las mismas a quien promovió el amparo, a los personados en el proceso, al Abogado del Estado, si estuviera interesada la Administración Pública, y al Ministerio Fiscal. La vista será por plazo común que no podrá exceder de veinte días, y durante él podrán presentarse las alegaciones procedentes.

Dos. Presentadas las alegaciones o transcurrido el plazo otorgado para efectuarlas, la Sala podrá deferir la resolución del recurso, cuando para su resolución sea aplicable doctrina consolidada del Tribunal Constitucional, a una de sus Secciones o señalar día para la vista, en su caso, o deliberación y votación.

Tres. La Sala, o en su caso la Sección, pronunciará la sentencia que proceda en el plazo de 10 días a partir del día señalado para la vista o deliberación.

CAPÍTULO III

De la resolución de los recursos de amparo constitucional y sus efectos

Artículo cincuenta y tres.

La Sala o, en su caso, la Sección, al conocer del fondo del asunto, pronunciará en su sentencia alguno de estos fallos:

a) Otorgamiento de amparo.
b) Denegación de amparo.

Artículo cincuenta y cuatro.

Cuando la Sala o, en su caso, la Sección conozca del recurso de amparo respecto de decisiones de jueces y tribunales, limitará su función a concretar si se han violado derechos o libertades del demandante y a preservar o restablecer estos derechos o libertades, y se abstendrá de cualquier otra consideración sobre la actuación de los órganos jurisdiccionales.

Artículo cincuenta y cinco.

Uno. La sentencia que otorgue el amparo contendrá alguno o algunos de los pronunciamientos siguientes:

a) Declaración de nulidad de la decisión, acto o resolución que hayan impedido el pleno ejercicio de los derechos o libertades protegidos, con determinación, en su caso, de la extensión de sus efectos.

b) Reconocimiento del derecho o libertad pública, de conformidad con su contenido constitucionalmente declarado.

c) Restablecimiento del recurrente en la integridad de su derecho o libertad con la adopción de las medidas apropiadas, en su caso, para su conservación.

Dos. En el supuesto de que el recurso de amparo debiera ser estimado porque, a juicio de la Sala o, en su caso, la Sección, la ley aplicada lesione derechos fundamentales o libertades públicas, se elevará la cuestión al Pleno con suspensión del plazo para dictar sentencia, de conformidad con lo prevenido en los artículos 35 y siguientes.

Artículo cincuenta y seis.

1. La interposición del recurso de amparo no suspenderá los efectos del acto o sentencia impugnados.

2. Ello no obstante, cuando la ejecución del acto o sentencia impugnados produzca un perjuicio al recurrente que pudiera hacer perder al amparo su finalidad, la Sala, o la Sección

en el supuesto del artículo 52.2, de oficio o a instancia del recurrente, podrá disponer la suspensión, total o parcial, de sus efectos, siempre y cuando la suspensión no ocasione perturbación grave a un interés constitucionalmente protegido, ni a los derechos fundamentales o libertades de otra persona.

3. Asimismo, la Sala o la Sección podrá adoptar cualesquiera medidas cautelares y resoluciones provisionales previstas en el ordenamiento, que, por su naturaleza, puedan aplicarse en el proceso de amparo y tiendan a evitar que el recurso pierda su finalidad.

4. La suspensión u otra medida cautelar podrá pedirse en cualquier tiempo, antes de haberse pronunciado la sentencia o decidirse el amparo de otro modo. El incidente de suspensión se sustanciará con audiencia de las partes y del Ministerio Fiscal, por un plazo común que no excederá de tres días y con el informe de las autoridades responsables de la ejecución, si la Sala o la Sección lo creyera necesario. La Sala o la Sección podrá condicionar la denegación de la suspensión en el caso de que pudiera seguirse perturbación grave de los derechos de un tercero, a la constitución de caución suficiente para responder de los daños o perjuicios que pudieran originarse.

5. La Sala o la Sección podrá condicionar la suspensión de la ejecución y la adopción de las medidas cautelares a la satisfacción por el interesado de la oportuna fianza suficiente para responder de los daños y perjuicios que pudieren originarse. Su fijación y determinación podrá delegarse en el órgano jurisdiccional de instancia.

6. En supuestos de urgencia excepcional, la adopción de la suspensión y de las medidas cautelares y provisionales podrá efectuarse en la resolución de la admisión a trámite. Dicha adopción podrá ser impugnada en el plazo de cinco días desde su notificación, por el Ministerio Fiscal y demás partes personadas. La Sala o la Sección resolverá el incidente mediante auto no susceptible de recurso alguno.

Artículo cincuenta y siete.

La suspensión o su denegación puede ser modificada durante el curso del juicio de amparo constitucional, de oficio o a instancia de parte, en virtud de circunstancias sobrevenidas o que no pudieron ser conocidas al tiempo de sustanciarse el incidente de suspensión.

Artículo cincuenta y ocho.

Uno. Serán competentes para resolver sobre las peticiones de indemnización de los daños causados como consecuencia de la concesión o denegación de la suspensión los Jueces o Tribunales, a cuya disposición se pondrán las fianzas constituidas.

Dos. Las peticiones de indemnización, que se sustanciarán por el trámite de los incidentes, deberán presentarse dentro del plazo de un año a partir de la publicación de la sentencia del Tribunal Constitucional.

TÍTULO IV

De los conflictos constitucionales

CAPÍTULO I

Disposiciones generales

Artículo cincuenta y nueve.

1. El Tribunal Constitucional entenderá de los conflictos que se susciten sobre las competencias o atribuciones asignadas directamente por la Constitución, los Estatutos de Autonomía o las leyes orgánicas u ordinarias dictadas para delimitar los ámbitos propios del Estado y las Comunidades Autónomas y que opongan:

a) Al Estado con una o más Comunidades Autónomas.
b) A dos o más Comunidades Autónomas entre sí.

c) Al Gobierno con el Congreso de los Diputados, el Senado o el Consejo General del Poder Judicial; o a cualquiera de estos órganos constitucionales entre sí.

2. El Tribunal Constitucional entenderá también de los conflictos en defensa de la autonomía local que planteen los municipios y provincias frente al Estado o a una Comunidad Autónoma.

CAPÍTULO II

De los conflictos entre el Estado y las Comunidades Autónomas o de éstas entre sí

Artículo sesenta.

Los conflictos de competencia que opongan al Estado con una Comunidad Autónoma o a éstas entre sí, podrán ser suscitados por el Gobierno o por los órganos colegiados ejecutivos de las Comunidades Autónomas, en la forma que determinan los artículos siguiente. Los conflictos negativos podrán ser instados también por las personas físicas o jurídicas interesadas.

Artículo sesenta y uno.

Uno. Pueden dar lugar al planteamiento de los conflictos de competencia las disposiciones, resoluciones y actos emanados de los órganos del Estado o de los órganos de las Comunidades Autónomas o la omisión de tales disposiciones, resoluciones o actos.

Dos. Cuando se plantease un conflicto de los mencionados en el artículo anterior con motivo de una disposición, resolución o acto cuya impugnación estuviese pendiente ante cualquier Tribunal, este suspenderá el curso del proceso hasta la decisión del conflicto constitucional.

Tres. La decisión del Tribunal Constitucional vinculará a todos los poderes públicos y tendrá plenos efectos frente a todos.

Sección primera. Conflictos positivos

Artículo sesenta y dos.

Cuando el Gobierno considere que una disposición o resolución de una Comunidad Autónoma no respeta el orden de competencia establecido en la Constitución, en los Estatutos de Autonomía o en las Leyes orgánicas correspondientes, podrá formalizar directamente ante el Tribunal Constitucional, en el plazo de dos meses, el conflicto de competencia, o hacer uso del previo requerimiento regulado en el artículo siguiente, todo ello sin perjuicio de que el Gobierno pueda invocar el artículo ciento sesenta y uno, dos, de la Constitución, con los efectos correspondientes.

Artículo sesenta y tres.

Uno. Cuando el órgano ejecutivo superior de una Comunidad Autónoma considerase que una disposición, resolución o acto emanado de la autoridad de otra Comunidad o del Estado no respeta el orden de competencias establecido en la Constitución, en los Estatutos de Autonomía o en las Leyes correspondientes y siempre que afecte a su propio ámbito, requerirá a aquélla o a éste para que sea derogada la disposición o anulados la resolución o el acto en cuestión.

Dos. El requerimiento de incompetencia podrá formularse dentro de los dos meses siguientes al día de la publicación o comunicación de la disposición, resolución o acto que se entiendan viciados de incompetencia o con motivo de un acto concreto de aplicación y se dirigirá directamente al Gobierno o al órgano ejecutivo superior de la otra Comunidad Autónoma, dando cuenta igualmente al Gobierno en este caso.

Tres. En el requerimiento se especificarán con claridad los preceptos de la disposición o los puntos concretos de la resolución o acto viciados de incompetencia, así como las disposiciones legales o constitucionales de las que el vicio resulte.

Cuatro. El órgano requerido, si estima fundado el requerimiento, deberá atenderlo en el plazo máximo de un mes a partir de su recepción, comunicándolo así al requirente y al Gobierno, si éste no actuara en tal condición. Si no lo estimara fundado, deberá igualmente rechazarlo dentro del mismo plazo, a cuyo término se entenderán en todo caso rechazados los requerimientos no atendidos.

Cinco. Dentro del mes siguiente a la notificación del rechazo o al término del plazo a que se refiere el apartado anterior, el órgano requirente, si no ha obtenido satisfacción, podrá plantear el conflicto ante el Tribunal Constitucional, certificando el cumplimiento infructuoso del trámite de requerimiento y alegando los fundamentos jurídicos en que éste se apoya.

Artículo sesenta y cuatro.

Uno. En el término de diez días, el Tribunal comunicará al Gobierno u órgano autonómico correspondiente la iniciación del conflicto, señalándose plazo, que en ningún caso será mayor de veinte días, para que aporte cuantos documentos y alegaciones considere convenientes.

Dos. Si el conflicto hubiere sido entablado por el Gobierno una vez adoptada decisión por la Comunidad Autónoma y con invocación del artículo ciento sesenta y uno, dos. de la Constitución, su formalización comunicada por el Tribunal suspenderá inmediatamente la vigencia de la disposición, resolución o acto que hubiesen dado origen al conflicto.

Tres. En los restantes supuestos, el órgano que formalice el conflicto podrá solicitar del Tribunal la suspensión de la disposición, resolución o acto objeto del conflicto, invocando perjuicios de imposible o difícil reparación, el Tribunal acordará o denegará libremente la supension solicitada.

Cuatro. El planteamiento del conflicto iniciado por el Gobierno y, en su caso, el auto del Tribunal por el que se acuerde la suspensión de la disposición, resolución o acto objeto del conflicto serán notificados a los interesados y publicados en el correspondiente «Diario Oficial» por el propio Tribunal.

Artículo sesenta y cinco.

Uno. El Tribunal podrá solicitar de las partes cuantas informaciones, aclaraciones o precisiones juzgue necesarias para su decisión y resolverá dentro de los quince días siguientes al término del plazo de alegaciones o del que, en su caso, se fijare para las informaciones, aclaraciones o precisiones complementarias antes aludidas.

Dos. En el caso previsto en el número dos del artículo anterior, si la sentencia no se produjera dentro de los cinco meses desde la iniciación del conflicto, el Tribunal deberá resolver dentro de este plazo, por auto motivado, acerca del mantenimiento o levantamiento de la suspensión del acto, resolución o disposición impugnados de incompetencia por el Gobierno.

Artículo sesenta y seis.

La sentencia declarará la titularidad de la competencia controvertida y acordará, en su caso, la anulación de la disposición, resolución o actos que originaron el conflicto en cuanto estuvieren viciados de incompetencia, pudiendo disponer lo que fuera procedente respecto de las situaciones de hecho o de derecho creadas al amparo de la misma.

Artículo sesenta y siete.

Si la competencia controvertida hubiera sido atribuida por una Ley o norma con rango de Ley, el conflicto de competencias se tramitará desde su inicio o, en su caso, desde que en defensa de la competencia ejercida se invocare la existencia de la norma legal habilitante, en la forma prevista para el recurso de inconstitucionalidad.

Sección segunda. Conflictos negativos

Artículo sesenta y ocho.

Uno. En el caso de que un órgano de la Administración del Estado declinare su competencia para resolver cualquier pretensión deducida ante el mismo por persona física o jurídica, por entender que la competencia corresponde a una Comunidad Autónoma, el interesado, tras haber agotado la vía administrativa mediante recurso ante el Ministerio correspondiente, podrá reproducir su pretensión ante el órgano ejecutivo colegiado de la Comunidad Autónoma que la resolución declare competente. De análogo modo se procederá si la solicitud se promueve ante una Comunidad Autónoma y ésta se inhibe por entender competente al Estado o a otra Comunidad Autónoma.

Dos. La Administración solicitada en segundo lugar deberá admitir o declinar su competencia en el plazo de un mes. Si la admitiere, procederá a tramitar la solicitud presentada. Si se inhibiere, deberá notificarlo al requirente, con indicación precisa de los preceptos en que se funda su resolución.

Tres. Si la Administración a que se refiere el apartado anterior declinare su competencia o no pronunciare decisión afirmativa en el plazo establecido, el interesado podrá acudir al Tribunal Constitucional. A tal efecto, deducirá la oportuna demanda dentro del mes siguiente a la notificación de la declinatoria, o si trascurriese el plazo establecido en el apartado dos del presente artículo sin resolución expresa, en solicitud de que se tramite y resuelva el conflicto de competencia negativo.

Artículo sesenta y nueve.

Uno. La solicitud de planteamiento de conflicto se formulará mediante escrito, al que habrán de acompañarse los documentos que acrediten haber agotado el trámite a que se refiere el artículo anterior y las resoluciones recaídas durante el mismo.

Dos. Si el Tribunal entendiere que la negativa de las Administraciones implicadas se basa precisamente en una diferencia de interpretación de preceptos constitucionales o de los Estatutos de Autonomía o de Leyes orgánicas u ordinarias que delimiten los ámbitos de competencia del Estado y de las Comunidades Autónomas declarará, mediante auto que habrá de ser dictado dentro de los diez días siguientes al de la presentación del escrito, planteado el conflicto. Dará inmediato traslado del auto al solicitante y a las Administraciones implicadas, así como a cualesquiera otras que el Tribunal considere competentes, a las que remitirá además copia de la solicitud de su planteamiento y de los documentos acompañados a la misma y fijará a todos el plazo común de un mes para que aleguen cuanto estimen conducente a la solución del conflicto planteado.

Artículo setenta.

Uno. Dentro del mes siguiente a la conclusión del plazo señalado en el artículo anterior o, en su caso, del que sucesivamente el Tribunal hubiere concedido para responder a las peticiones de aclaración, ampliación o precisión que les hubiere dirigido, se dictará sentencia que declarará cuál es la Administración competente.

Dos. Los plazos administrativos agotados se entenderán nuevamente abiertos por su duración ordinaria a partir de la publicación de la sentencia.

Artículo setenta y uno.

Uno. El Gobierno podrá igualmente plantear conflicto de competencias negativo cuando habiendo requerido al órgano ejecutivo superior de una Comunidad Autónoma para que ejercite las atribuciones propias de la competencia que a la Comunidad confieran sus propios estatutos o una Ley orgánica de delegación o transferencia, sea desatendido su requerimiento por declararse incompetente el órgano requerido.

Dos. La declaración de incompetencia se entenderá implícita por la simple inactividad del órgano ejecutivo requerido dentro del plazo que el Gobierno le hubiere fijado para el ejercicio de sus atribuciones, que en ningún caso será inferior a un mes.

Artículo setenta y dos.

Uno. Dentro del mes siguiente al día en que de manera expresa o tácita haya de considerarse rechazado el requerimiento a que se refiere el artículo anterior, el Gobierno podrá plantear ante el Tribunal Constitucional el conflicto negativo mediante escrito en el que habrán de indicarse los preceptos constitucionales, estatutarios o legales que a su juicio obligan a la Comunidad Autónoma a ejercer sus atribuciones.

Dos. El Tribunal dará traslado del escrito al órgano ejecutivo superior de la Comunidad Autónoma, al que fijará un plazo de un mes para presentar las alegaciones que entienda oportunas.

Tres. Dentro del mes siguiente a la conclusión de tal plazo o, en su caso, del que sucesivamente hubiere fijado al Estado o a la Comunidad Autónoma para responder a las peticiones de aclaración, ampliación o precisiones que les hubiere dirigido, el Tribunal dictará sentencia, que contendrá alguno de los siguientes pronunciamientos:

a) La declaración de que el requerimiento es procedente, que conllevará el establecimiento de un plazo dentro del cual la Comunidad Autónoma deberá ejercitar la atribución requerida.

b) La declaración de que el requerimiento es improcedente.

CAPÍTULO III

De los conflictos entre órganos constitucionales del Estado

Artículo setenta y tres.

Uno. En el caso en que alguno de los órganos constitucionales a los que se refiere el artículo 59.3(*) de esta Ley, por acuerdo de sus respectivos Plenos, estime que otro de dichos órganos adopta decisiones asumiendo atribuciones que la Constitución o las Leyes orgánicas confieren al primero, éste se lo hará saber así dentro del mes siguiente a la fecha en que llegue a su conocimiento la decisión de la que se infiera la indebida asunción de atribuciones y solicitará de él que la revoque.

(*) En la actualidad, artículo 59.1.c), conforme a la redacción dada por la Ley Orgánica 7/1999, de 21 de abril (Ref. BOE-A-1999-8927).

Dos. Si el órgano al que se dirige la notificación afirmara que actúa en el ejercicio constitucional y legal de sus atribuciones o, dentro del plazo de un mes a partir de la recepción de aquella no rectificase en el sentido que le hubiera sido solicitado, el órgano que estime indebidamente asumidas sus atribuciones planteará el conflicto ante el Tribunal Constitucional dentro del mes siguiente. A tal efecto, presentará un escrito en el que se especificarán los preceptos que considera vulnerados y formulará las alegaciones que estime oportunas. A este escrito acompañará una certificación de los antecedentes que repute necesarios y de la comunicación cursada en cumplimiento de lo prevenido en el apartado anterior de este artículo.

Artículo setenta y cuatro.

Recibido el escrito, el Tribunal, dentro de los diez días siguientes, dará traslado del mismo al órgano requerido y le fijará el plazo de un mes para formular las alegaciones que estime procedentes. Idénticos traslados y emplazamientos se harán a todos los demás órganos legitimados para plantear este género de conflictos, los cuales podrán comparecer en el procedimiento, en apoyo del demandante o del demandado, si entendieren que la solución del conflicto planteado afecta de algún modo a sus propias atribuciones.

Artículo setenta y cinco.

Uno. El Tribunal podrá solicitar de las partes cuantas informaciones, aclaraciones o precisiones juzgue necesarias para su decisión y resolverá dentro del mes siguiente a la expiración del plazo de alegaciones a que se refiere el artículo anterior o del que, en su

caso, se fijare para las informaciones, aclaraciones o precisiones complementarias, que no será superior a otros treinta días.

Dos. La sentencia del Tribunal determinará a qué órgano corresponden las atribuciones constitucionales controvertidas y declarará nulos los actos ejecutados por invasión de atribuciones y resolverá, en su caso, lo que procediere sobre las situaciones jurídicas producidas al amparo de los mismos.

CAPÍTULO IV

De los conflictos en defensa de la autonomía local

Artículo setenta y cinco bis.

1. Podrán dar lugar al planteamiento de los conflictos en defensa de la autonomía local las normas del Estado con rango de ley o las disposiciones con rango de ley de las Comunidades Autónomas que lesionen la autonomía local constitucionalmente garantizada.

2. La decisión del Tribunal Constitucional vinculará a todos los poderes públicos y tendrá plenos efectos frente a todos.

Artículo setenta y cinco ter.

1. Están legitimados para plantear estos conflictos:

a) El municipio o provincia que sea destinatario único de la ley.

b) Un número de municipios que supongan al menos un séptimo de los existentes en el ámbito territorial de aplicación de la disposición con rango de ley, y representen como mínimo un sexto de la población oficial del ámbito territorial correspondiente.

c) Un número de provincias que supongan al menos la mitad de las existentes en el ámbito territorial de aplicación de la disposición con rango de ley, y representen como mínimo la mitad de la población oficial.

2. Para iniciar la tramitación de los conflictos en defensa de la autonomía local será necesario el acuerdo del órgano plenario de las Corporaciones locales con el voto favorable de la mayoría absoluta del número legal de miembros de las mismas.

3. Una vez cumplido el requisito establecido en el apartado anterior, y de manera previa a la formalización del conflicto, deberá solicitarse dictamen, con carácter preceptivo pero no vinculante, del Consejo de Estado u órgano consultivo de la correspondiente Comunidad Autónoma, según que el ámbito territorial al que pertenezcan las Corporaciones locales corresponda a variasoauna Comunidad Autónoma. En las Comunidades Autónomas que no dispongan de órgano consultivo, el dictamen corresponderá al Consejo de Estado.

4. Las asociaciones de entidades locales podrán asistir a los entes locales legitimados a fin de facilitarles el cumplimiento de los requisitos establecidos en el procedimiento de tramitación del presente conflicto.

Artículo setenta y cinco quater.

1. La solicitud de los dictámenes a que se refiere el artículo anterior deberá formalizarse dentro de los tres meses siguientes al día de la publicación de la ley que se entienda lesiona la autonomía local.

2. Dentro del mes siguiente a la recepción del dictamen del Consejo de Estado o del órgano consultivo de la correspondiente Comunidad Autónoma, los municipios o provincias legitimados podrán plantear el conflicto ante el Tribunal Constitucional, acreditando el cumplimiento de los requisitos exigidos en el artículo anterior y alegándose los fundamentos jurídicos en que se apoya.

Artículo setenta y cinco quinquies.

1. Planteado el conflicto, el Tribunal podrá acordar, mediante auto motivado, la inadmisión del mismo por falta de legitimación u otros requisitos exigibles y no subsanables o cuando estuviere notoriamente infundada la controversia suscitada.

2. Admitido a trámite el conflicto, en el término de diez días, el Tribunal dará traslado del mismo a los órganos legislativo y ejecutivo de la Comunidad Autónoma de quien hubiese emanado la ley, y en todo caso a los órganos legislativo y ejecutivo del Estado. La personación y la formulación de alegaciones deberán realizarse en el plazo de veinte días.

3. El planteamiento del conflicto será notificado a los interesados y publicado en el correspondiente Diario Oficial por el propio Tribunal.

4. El Tribunal podrá solicitar de las partes cuantas informaciones, aclaraciones o precisiones juzgue necesarias para su decisión y resolverá dentro de los quince días siguientes al término del plazo de alegaciones o del que, en su caso, se fijare para las informaciones, aclaraciones o precisiones complementarias antes aludidas.

5. La sentencia declarará si existe o no vulneración de la autonomía local constitucionalmente garantizada, determinando, según proceda, la titularidad o atribución de la competencia controvertida, y resolverá, en su caso, lo que procediere sobre las situaciones de hecho o de derecho creadas en lesión de la autonomía local.

6. La declaración, en su caso, de inconstitucionalidad de la ley que haya dado lugar al conflicto requerirá nueva sentencia si el Pleno decide plantearse la cuestión tras la resolución del conflicto declarando que ha habido vulneración de la autonomía local. La cuestión se sustanciará por el procedimiento establecido en los artículos 37 y concordantes y tendrá los efectos ordinarios previstos en los artículos 38 y siguientes.

TÍTULO V

De la impugnación de disposiciones sin fuerza de Ley y resoluciones de las Comunidades Autónomas prevista en el artículo 161.2 de la Constitución

Artículo setenta y seis.

Dentro de los dos meses siguientes a la fecha de su publicación o, en defecto de la misma, desde que llegare a su conocimiento, el Gobierno podrá impugnar ante el Tribunal Constitucional las disposiciones normativas sin fuerza de Ley y resoluciones emanadas de cualquier órgano de las Comunidades Autónomas.

Artículo setenta y siete.

La impugnación regulada en este título, sea cual fuere el motivo en que se base, se formulará y sustanciará por el procedimiento previsto en los artículos sesenta y dos a sesenta y siete de esta Ley. La formulación de la impugnación comunicada por el Tribunal producirá la suspensión de la disposición o resolución recurrida hasta que el Tribunal resuelva ratificarla o levantarla en plazo no superior a cinco meses, salvo que, con anterioridad, hubiera dictado sentencia.

TÍTULO VI

De la declaración sobre la constitucionalidad de los tratados internacionales

Artículo setenta y ocho.

Uno. El Gobierno o cualquiera de ambas Cámaras podrán requerir al Tribunal Constitucional para que se pronuncie sobre la existencia o inexistencia de contradicción entre la Constitución y las estipulaciones de un tratado internacional cuyo texto estuviera ya definitivamente fijado, pero al que no se hubiere prestado aún el consentimiento del Estado.

Dos. Recibido el requerimiento, el Tribunal Constitucional emplazará al solicitante y a los restantes órganos legitimados, según lo previsto en el apartado anterior, a fin de que, en el término de un mes, expresen su opinión fundada sobre la cuestión. Dentro del mes siguiente al transcurso de este plazo y salvo lo dispuesto en el apartado siguiente, el Tribunal Constitucional emitirá su declaración, que, de acuerdo con lo establecido en el artículo noventa y cinco de la Constitución, tendrá carácter vinculante.

Tres. En cualquier momento podrá el Tribunal Constitucional solicitar de los órganos mencionados en el apartado anterior o de otras personas físicas o jurídicas u otros órganos del Estado o de las Comunidades Autónomas, cuantas aclaraciones, ampliaciones o precisiones estimen necesarias, alargando el plazo de un mes antes citado en el mismo tiempo que hubiese concedido para responder a sus consultas, que no podrá exceder de treinta días.

TÍTULO VI BIS.

Del recurso previo de inconstitucionalidad contra Proyectos de Estatutos de Autonomía y contra Propuestas de Reforma de Estatutos de Autonomía

Artículo setenta y nueve.

Uno. Son susceptibles de recurso de inconstitucionalidad, con carácter previo, los Proyectos de Estatutos de Autonomía y las propuestas de reforma de los mismos.

Dos. El recurso tendrá por objeto la impugnación del texto definitivo del Proyecto de Estatuto o de la Propuesta de Reforma de un Estatuto, una vez aprobado por las Cortes Generales.

Tres. Están legitimados para interponer el recurso previo de inconstitucionalidad quienes, de acuerdo con la Constitución y con esta Ley Orgánica, están legitimados para interponer recursos de inconstitucionalidad contra Estatutos de Autonomía.

Cuatro. El plazo para la interposición del recurso será de tres días desde la publicación del texto aprobado en el «Boletín Oficial de las Cortes Generales». La interposición del recurso suspenderá automáticamente todos los trámites subsiguientes.

Cinco. Cuando la aprobación del Proyecto de Estatuto o de la Propuesta de reforma haya de ser sometida a referéndum en el territorio de la respectiva Comunidad Autónoma, el mismo no podrá convocarse hasta que haya resuelto el Tribunal Constitucional y, en su caso, se hayan suprimido o modificado por las Cortes Generales los preceptos declarados inconstitucionales.

Seis. El recurso previo de inconstitucionalidad se sustanciará en la forma prevista en el capítulo II del título II de esta Ley y deberá ser resuelto por el Tribunal Constitucional en el plazo improrrogable de seis meses desde su interposición. El Tribunal dispondrá lo necesario para dar cumplimiento efectivo a esta previsión, reduciendo los plazos ordinarios y dando en todo caso preferencia a la resolución de estos recursos sobre el resto de asuntos en tramitación.

Siete. Cuando el pronunciamiento del Tribunal declare la inexistencia de la inconstitucionalidad alegada, seguirán su curso los trámites conducentes a su entrada en vigor, incluido, en su caso, el correspondiente procedimiento de convocatoria y celebración de referéndum.

Ocho. Si, por el contrario, declara la inconstitucionalidad del texto impugnado, deberá concretar los preceptos a los que alcanza, aquellos que por conexión o consecuencia quedan afectados por tal declaración y el precepto o preceptos constitucionales infringidos. En este supuesto, la tramitación no podrá proseguir sin que tales preceptos hayan sido suprimidos o modificados por las Cortes Generales.

Nueve. El pronunciamiento en el recurso previo no prejuzga la decisión del Tribunal en los recursos o cuestiones de inconstitucionalidad que pudieren interponerse tras la entrada en vigor con fuerza de ley del texto impugnado en la vía previa.

TÍTULO VII

De las disposiciones comunes sobre procedimiento

Artículo ochenta.

Se aplicarán, con carácter supletorio de la presente Ley, los preceptos de la Ley Orgánica del Poder Judicial y de la Ley de Enjuiciamiento Civil, en materia de comparecencia en juicio, recusación y abstención, publicidad y forma de los actos,

comunicaciones y actos de auxilio jurisdiccional, día y horas hábiles, cómputo de plazos, deliberación y votación, caducidad, renuncia y desistimiento, lengua oficial y policía de estrados.

En materia de ejecución de resoluciones se aplicará, con carácter supletorio de la presente Ley, los preceptos de la Ley de la Jurisdicción Contencioso-administrativa.

Artículo ochenta y uno.

Uno. Las personas físicas o jurídicas cuyo interés les legitime para comparecer en los procesos constitucionales, como actores o coadyuvantes, deberán conferir su representación a un Procurador y actuar bajo la dirección de Letrado. Podrán comparecer por sí mismas, para defender derechos o intereses propios, las personas que tengan título de Licenciado en Derecho, aunque no ejerzan la profesión de Procurador o de Abogado.

Dos. Para ejercer ante el Tribunal Constitucional en calidad de Abogado, se requerirá estar incorporado a cualquiera de los Colegios de Abogados de España en calidad de ejerciente.

Tres. Estarán inhabilitados para actuar como Abogado ante el Tribunal Constitucional quienes hubieren sido Magistrados o Letrados del mismo.

Artículo ochenta y dos.

Uno. Los órganos o el conjunto de Diputados o Senadores investidos por la Constitución y por esta Ley de legitimación para promover procesos constitucionales actuarán en los mismos representados por el miembro o miembros que designen o por un comisionado nombrado al efecto.

Dos. Los órganos ejecutivos, tanto del Estado como de las Comunidades autónomas, serán representados y defendidos por sus Abogados. Por los órganos ejecutivos del Estado actuará el Abogado del Estado.

Artículo ochenta y tres.

El Tribunal podrá, a instancia de parte o de oficio, en cualquier momento, y previa audiencia de los comparecidos en el proceso constitucional, disponer la acumulación de aquellos procesos con objetos conexos que justifiquen la unidad de tramitación y decisión. La audiencia se hará por plazo que no exceda de diez días.

Artículo ochenta y cuatro.

El Tribunal, en cualquier tiempo anterior a la decisión, podrá comunicar a los comparecidos en el proceso constitucional la eventual existencia de otros motivos distintos de los alegados, con relevancia para acordar lo procedente sobre la admisión o inadmisión y, en su caso, sobre la estimación o desestimación de la pretensión constitucional. La audiencia será común, por plazo no superior al de diez días con suspensión del término para dictar la resolución que procediere.

Artículo ochenta y cinco.

Uno. La iniciación de un proceso constitucional deberá hacerse por escrito fundado en el que se fijará con precisión y claridad lo que se pida.

Dos. Los escritos de iniciación del proceso se presentarán en la sede del Tribunal Constitucional dentro del plazo legalmente establecido. Los recursos de amparo podrán también presentarse hasta las 15 horas del día hábil siguiente al del vencimiento del plazo de interposición, en el registro del Tribunal Constitucional, o en la oficina o servicio de registro central de los tribunales civiles de cualquier localidad, de conformidad con lo establecido en el artículo 135.1 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

El Tribunal determinará reglamentariamente las condiciones de empleo, a los efectos anteriores, de cualesquiera medios técnicos, electrónicos, informáticos o telemáticos.

Tres. El Pleno o las Salas podrán acordar la celebración de vista oral.

Artículo ochenta y seis.

Uno. La decisión del proceso constitucional se producirá en forma de sentencia. Sin embargo, las decisiones de inadmisión inicial, desistimiento y caducidad adoptarán la forma de auto salvo que la presente Ley disponga expresamente otra forma. Las otras resoluciones adoptarán la forma de auto si son motivadas o de providencia si no lo son, según la índole de su contenido.

Dos. Las sentencias y las declaraciones a que se refiere el título VI se publicarán en el "Boletín Oficial del Estado" dentro de los 30 días siguientes a la fecha del fallo. También podrá el Tribunal ordenar la publicación de sus autos en la misma forma cuando así lo estime conveniente.

Tres. Sin perjuicio en lo dispuesto en el apartado anterior, el Tribunal podrá disponer que las sentencias y demás resoluciones dictadas sean objeto de publicación a través de otros medios, y adoptará, en su caso, las medidas que estime pertinentes para la protección de los derechos reconocidos en el artículo 18.4 de la Constitución.

Artículo ochenta y siete.

1. Todos los poderes públicos están obligados al cumplimiento de lo que el Tribunal Constitucional resuelva.

En particular, el Tribunal Constitucional podrá acordar la notificación personal de sus resoluciones a cualquier autoridad o empleado público que se considere necesario.

2. Los Juzgados y Tribunales prestarán con carácter preferente y urgente al Tribunal Constitucional el auxilio jurisdiccional que éste solicite.

A estos efectos, las sentencias y resoluciones del Tribunal Constitucional tendrán la consideración de títulos ejecutivos.

Artículo ochenta y ocho.

Uno. El Tribunal Constitucional podrá recabar de los poderes públicos y de los órganos de cualquier Administración Pública la remisión del expediente y de los informes y documentos relativos a la disposición o acto origen del proceso constitucional. Si el recurso hubiera sido ya admitido, el Tribunal habilitará un plazo para que el expediente, la información o los documentos puedan ser conocidos por las partes para que éstas aleguen lo que a su derecho convenga.

Dos. El Tribunal dispondrá las medidas necesarias para preservar el secreto que legalmente afecte a determinada documentación y el que por decisión motivada acuerde para determinadas actuaciones.

Artículo ochenta y nueve.

Uno. El Tribunal, de oficio o a instancia de parte, podrá acordar la práctica de prueba cuando lo estimare necesario y resolverá libremente sobre la forma y el tiempo de su realización, sin que en ningún caso pueda exceder de treinta días.

Dos. Si un testigo, citado por el Tribunal, sólo puede comparecer con autorización superior, la autoridad competente para otorgarla expondrá al Tribunal, en su caso, las razones que justifican su denegación. El Tribunal, oído este informe, resolverá en definitiva.

Artículo noventa.

Uno. Salvo en los casos para los que esta Ley establece otros requisitos, las decisiones se adoptarán por la mayoría de los miembros del Pleno, Sala o Sección que participen en la deliberación. En caso de empate, decidirá el voto del Presidente.

Dos. El Presidente y los Magistrados del Tribunal podrán reflejar en voto particular su opinión discrepante, siempre que haya sido defendida en la deliberación, tanto por lo que se refiere a la decisión como a la fundamentación. Los votos particulares se incorporarán a la resolución y cuando se trate de sentencias, autos o declaraciones se publicarán con éstas en el "Boletín Oficial del Estado".

Artículo noventa y uno.

El Tribunal podrá suspender el procedimiento que se sigue ante el mismo hasta la resolución de un proceso penal pendiente ante un juzgado o Tribunal de este orden.

Artículo noventa y dos.

1. El Tribunal Constitucional velará por el cumplimiento efectivo de sus resoluciones. Podrá disponer en la sentencia, o en la resolución, o en actos posteriores, quién ha de ejecutarla, las medidas de ejecución necesarias y, en su caso, resolver las incidencias de la ejecución.

Podrá también declarar la nulidad de cualesquiera resoluciones que contravengan las dictadas en el ejercicio de su jurisdicción, con ocasión de la ejecución de éstas, previa audiencia del Ministerio Fiscal y del órgano que las dictó.

2. El Tribunal podrá recabar el auxilio de cualquiera de las administraciones y poderes públicos para garantizar la efectividad de sus resoluciones que lo prestarán con carácter preferente y urgente.

3. Las partes podrán promover el incidente de ejecución previsto en el apartado 1, para proponer al Tribunal las medidas de ejecución necesarias para garantizar el cumplimiento efectivo de sus resoluciones.

4. En caso de advertirse que una resolución dictada en el ejercicio de su jurisdicción pudiera estar siendo incumplida, el Tribunal, de oficio o a instancia de alguna de las partes del proceso en que hubiera recaído, requerirá a las instituciones, autoridades, empleados públicos o particulares a quienes corresponda llevar a cabo su cumplimiento para que en el plazo que se les fije informen al respecto.

Recibido el informe o transcurrido el plazo fijado, si el Tribunal apreciase el incumplimiento total o parcial de su resolución, podrá adoptar cualesquiera de las medidas siguientes:

a) Imponer multa coercitiva de tres mil a treinta mil euros a las autoridades, empleados públicos o particulares que incumplieren las resoluciones del Tribunal, pudiendo reiterar la multa hasta el cumplimiento íntegro de lo mandado.

b) Acordar la suspensión en sus funciones de las autoridades o empleados públicos de la Administración responsable del incumplimiento, durante el tiempo preciso para asegurar la observancia de los pronunciamientos del Tribunal.

c) La ejecución sustitutoria de las resoluciones recaídas en los procesos constitucionales. En este caso, el Tribunal podrá requerir la colaboración del Gobierno de la Nación a fin de que, en los términos fijados por el Tribunal, adopte las medidas necesarias para asegurar el cumplimiento de las resoluciones.

d) Deducir el oportuno testimonio de particulares para exigir la responsabilidad penal que pudiera corresponder.

5. Si se tratara de la ejecución de las resoluciones que acuerden la suspensión de las disposiciones, actos o actuaciones impugnadas y concurrieran circunstancias de especial transcendencia constitucional, el Tribunal, de oficio o a instancia del Gobierno, adoptará las medidas necesarias para asegurar su debido cumplimiento sin oír a las partes. En la misma resolución dará audiencia a las partes y al Ministerio Fiscal por plazo común de tres días, tras el cual el Tribunal dictará resolución levantando, confirmando o modificando las medidas previamente adoptadas.

Artículo noventa y tres.

Uno. Contra las sentencias del Tribunal Constitucional no cabe recurso alguno, pero en el plazo de dos días a contar desde su notificación, las partes podrán solicitar la aclaración de las mismas.

Dos. Contra las providencias y los autos que dicte el Tribunal Constitucional sólo procederá, en su caso, el recurso de súplica, que no tendrá efecto suspensivo. El recurso podrá interponerse en el plazo de tres días y se resolverá, previa audiencia común de las partes por igual tiempo, en los dos siguientes.

Artículo noventa y cuatro.

El Tribunal, a instancia de parte o de oficio, deberá antes de pronunciar sentencia, subsanar o convalidar los defectos que hubieran podido producirse en el procedimiento.

Artículo noventa y cinco.

Uno. El procedimiento ante el Tribunal Constitucional es gratuito.

Dos. El Tribunal podrá imponer las costas que se derivaren de la tramitación del proceso a la parte o partes que hayan mantenido posiciones infundadas, si apreciare temeridad o mala fe.

Tres. El Tribunal podrá imponer a quien formulase recursos de inconstitucionalidad o de amparo, con temeridad o abuso de derecho, una sanción pecuniaria de 600 a 3.000 euros.

Cuatro. Los límites de la cuantía de estas sanciones o de las multas previstas en la letra a) del apartado 4 del artículo 92 podrán ser revisados, en todo momento, mediante ley ordinaria.

TÍTULO VIII

Del personal al servicio del Tribunal Constitucional

Artículo noventa y seis.

Uno. Son funcionarios al servicio del Tribunal Constitucional:

a) El Secretario General.
b) Los letrados.
c) Los secretarios de justicia.
d) Los demás funcionarios que sean adscritos al Tribunal Constitucional.

Dos. Este personal se rige por lo establecido en esta Ley y en el Reglamento que en su desarrollo se dicte, y, con carácter supletorio, en lo que sea aplicable por la legislación vigente para el personal al servicio de la Administración de Justicia.

Tres. Los cargos y funciones relacionados en este artículo son incompatibles con cualquier otra función, destino o cargo, así como con el ejercicio profesional y con la intervención en actividades industriales, mercantiles o profesionales, incluso las consultivas y las de asesoramiento. No obstante, podrán ejercer aquellas funciones docentes o de investigación que, a juicio del Tribunal, no resulten incompatibles con el mejor servicio de éste.

Artículo noventa y siete.

1. El Tribunal Constitucional estará asistido por letrados que podrán ser seleccionados mediante concurso-oposición entre funcionarios públicos que hayan accedido a un cuerpo o escala del grupo A en su condición de licenciados en derecho, de acuerdo con el reglamento del Tribunal, o ser libremente designados en régimen de adscripción temporal, por el mismo Tribunal, en las condiciones que establezca el reglamento, entre abogados, profesores de universidad, magistrados, fiscales o funcionarios públicos que hayan accedido a un cuerpo o escala del grupo A en su condición de Licenciados en Derecho. Los nombrados quedarán en su carrera de origen en situación de servicios especiales por todo el tiempo en que presten sus servicios en el Tribunal Constitucional.

2. Durante los tres años inmediatamente posteriores al cese en sus funciones, los letrados tendrán la incompatibilidad a que se refiere el artículo 81.3.

Artículo noventa y ocho.

El Tribunal Constitucional tendrá un Secretario General elegido por el Pleno y nombrado por el Presidente entre los letrados, cuya jefatura ejercerá sin perjuicio de las facultades que corresponden al Presidente, al Tribunal y a las Salas.

Artículo noventa y nueve.

1. Corresponde también al Secretario General, bajo la autoridad e instrucciones del Presidente:

a) La dirección y coordinación de los servicios del Tribunal y la jefatura de su personal.
b) La recopilación, clasificación y publicación de la doctrina constitucional del Tribunal.
c) La preparación, ejecución y liquidación de presupuesto, asistido por el personal técnico.
d) Las demás funciones que le atribuya el reglamento del Tribunal.

2. Las normas propias del Tribunal podrán prever supuestos de delegación de competencias administrativas del Presidente en el Secretario General. Del mismo modo podrá preverse la delegación de competencias propias del Secretario General.
3. Contra las resoluciones del Secretario General podrá interponerse recurso de alzada ante el Presidente, cuya decisión agotará la vía administrativa. Esta decisión será susceptible de ulterior recurso contencioso-administrativo.

Artículo cien.

El Tribunal tendrá el número de secretarios de justicia que determine su plantilla. Los secretarios de justicia procederán del Cuerpo de Secretarios Judiciales y las vacantes se cubrirán por concurso de méritos entre quienes pudieran ocupar plaza en el Tribunal Supremo.

Artículo ciento uno.

Los Secretarios de Justicia ejercerán en el Tribunal o en las Salas la fe pública judicial y desempeñarán, respecto del Tribunal o Sala a la que estén adscritos, las funciones que la legislación orgánica y procesal de los Juzgados y Tribunales atribuye a los Secretarios.

Artículo ciento dos.

El Tribunal Constitucional adscribirá a su servicio el personal de la Administración de Justicia y demás funcionarios en las condiciones que fije su reglamento. Podrá, asimismo, contratar personal en régimen laboral para el desempeño de puestos que no impliquen participación directa ni indirecta en el ejercicio de las atribuciones del Tribunal Constitucional, y cuyas funciones sean propias de oficios, auxiliares de carácter instrumental o de apoyo administrativo. La contratación de este personal laboral se realizará mediante procesos de selección ajustados a los principios de igualdad, mérito y capacidad.

DISPOSICIONES TRANSITORIAS

Primera.

Uno. Dentro de los tres meses siguientes a la fecha de la entrada en vigor de la presente Ley, el Congreso de los Diputados, el Senado, el Gobierno y el Consejo General del Poder Judicial elevarán al Rey las propuestas de designación de los Magistrados del Tribunal Constitucional. Este plazo se interrumpirá para las Cámaras por el tiempo correspondiente a los períodos intersesiones.
Dos. El Tribunal se constituirá dentro de los quince días siguientes a la fecha de publicación de los últimos nombramientos, si todas las propuestas se elevasen dentro del mismo período de sesiones. En otro caso se constituirá y comenzará a ejercer sus competencias, en los quince días siguientes, al término del período de sesiones dentro del que se hubiesen efectuado los ocho primeros nombramientos, cualquiera que sea la razón que motive la falta de nombramiento de la totalidad de los Magistrados previstos en el artículo quinto de esta Ley.
Tres. En el primer concurso-oposición la selección de los Letrados del Tribunal Constitucional se realizará por una Comisión del propio Tribunal designada por el Pleno de éste y presidida por el Presidente del Tribunal.

Segunda.

Uno. Los plazos previstos en esta Ley para interponer el recurso de inconstitucionalidad o de amparo o promover un conflicto constitucional comenzarán a contarse desde el día en que quede constituido el Tribunal de acuerdo con la disposición transitoria anterior, cuando las Leyes, disposiciones, resoluciones o actos que originen el recurso o conflicto fueran anteriores a aquella fecha y no hubieran agotado sus efectos.

Dos. En tanto no sean desarrolladas las previsiones del artículo cincuenta y tres, dos, de la Constitución para configurar el procedimiento judicial de protección de los derechos y libertades fundamentales se entenderá que la vía judicial previa a la interposición del recurso de amparo será la contencioso-administrativa ordinaria o la configurada en la Sección segunda de la Ley sesenta y dos/mil novecientos setenta y ocho, de veintiséis de diciembre, sobre protección jurisdiccional de los derechos fundamentales, a cuyos efectos el ámbito de la misma se entiende extendido a todos los derechos y libertades a que se refiere el expresado artículo cincuenta y tres, dos, de la Constitución.

Tercera.

Uno. Los sorteos a que se refiere la disposición transitoria novena de la Constitución se efectuarán dentro del cuarto mes anterior a la fecha en que se cumplen, respectivamente, los tres o los seis años de aquella otra en que se produjo la inicial designación de los Magistrados de Tribunal Constitucional.

Dos. No será aplicable la limitación establecida en el artículo dieciséis, dos, de esta Ley a los Magistrados del Tribunal que cesarán en sus cargos, en virtud de lo establecido en la disposición transitoria novena de la Constitución, a los tres años de su designación.

Cuarta.

El Gobierno habilitará los créditos necesarios para el funcionamiento del Tribunal Constitucional hasta que éste disponga de presupuesto propio.

Quinta.

En el caso de Navarra, y salvo que de conformidad con la disposición transitoria cuarta de la Constitución ejerciera su derecho a incorporarse al Consejo General Vasco o al régimen autonómico vasco que le sustituya, la legitimación para suscitar los conflictos previstos en el artículo segundo, uno, c), y para promover el recurso de inconstitucionalidad que el artículo treinta y dos confiere a los órganos de las Comunidades Autónomas se entenderá conferida a la Diputación y al Parlamento Foral de Navarra.

DISPOSICIONES ADICIONALES

Primera.

1. El número de letrados seleccionados mediante concurso-oposición a los que se refiere el artículo 97.1 no podrá exceder de 16.

2. La plantilla del personal del Tribunal Constitucional sólo podrá ser modificada a través de la Ley de Presupuestos Generales del Estado.

Segunda.

Uno. El Tribunal elaborará su presupuesto, que figurará como una sección dentro de los Presupuestos Generales del Estado .

Dos. El Secretario general, asistido de personal técnico, asumirá la preparación, ejecución y liquidación de presupuesto.

Tercera.

1. Las referencias a las provincias contenidas en esta Ley se entenderán realizadas a las islas en las Comunidades Autónomas de las Illes Balears y Canarias.

2. Además de los sujetos legitimados de acuerdo con el artículo 75 ter.1 lo estarán también, frente a leyes y disposiciones normativas con rango de Ley de la Comunidad Autónoma de Canarias, tres Cabildos, y de la Comunidad Autónoma de las Illes Balears, dos Consejos Insulares, aun cuando en ambos casos no se alcance el porcentaje de población exigido en dicho precepto.

Cuarta.

1. Los conflictos de competencia que se puedan suscitar entre las instituciones de la Comunidad Autónoma del País Vasco y las de cada uno de sus Territorios Históricos se regirán por lo dispuesto en el artículo 39 de su Estatuto de Autonomía.

2. En el ámbito de la Comunidad Autónoma del País Vasco, además de los sujetos legitimados a que se refiere el artículo 75 ter.1, lo estarán también, a los efectos de los conflictos regulados en el artículo 75 bis de esta Ley, las correspondientes Juntas Generales y las Diputaciones Forales de cada Territorio Histórico, cuando el ámbito de aplicación de la ley afecte directamente a dicha Comunidad Autónoma.

Quinta.

1. Corresponderá al Tribunal Constitucional el conocimiento de los recursos interpuestos contra las Normas Forales fiscales de los Territorios de Álava, Guipúzcoa y Vizcaya, dictadas en el ejercicio de sus competencias exclusivas garantizadas por la disposición adicional primera de la Constitución y reconocidas en el artículo 41.2.a) del Estatuto de Autonomía para el País Vasco (Ley Orgánica 31/1979, de 18 de diciembre).

El Tribunal Constitucional resolverá también las cuestiones que se susciten con carácter prejudicial por los órganos jurisdiccionales sobre la validez de las referidas disposiciones, cuando de ella dependa el fallo del litigio principal.

El parámetro de validez de las Normas Forales enjuiciadas se ajustará a lo dispuesto en el artículo veintiocho de esta Ley.

2. La interposición y sus efectos, la legitimación, tramitación y sentencia de los recursos y cuestiones referidos en el apartado anterior, se regirá por lo dispuesto en el Título II de esta Ley para los recursos y cuestiones de inconstitucionalidad respectivamente.

Los trámites regulados en los artículos 34 y 37 se entenderán en su caso con las correspondientes Juntas Generales y Diputaciones Forales.

En la tramitación de los recursos y cuestiones regulados en esta disposición adicional se aplicarán las reglas atributivas de competencia al Pleno y a las Salas de los artículos diez y once de esta Ley.

3. Las normas del Estado con rango de ley podrán dar lugar al planteamiento de conflictos en defensa de la autonomía foral de los Territorios Históricos de la Comunidad Autónoma del País Vasco, constitucional y estatutariamente garantizada.

Están legitimadas para plantear estos conflictos las Diputaciones Forales y las Juntas Generales de los Territorios Históricos de Álava, Bizkaia y Gipuzkoa, mediante acuerdo adoptado al efecto.

Los referidos conflictos se tramitarán y resolverán con arreglo al procedimiento establecido en los artículos 63 y siguientes de esta Ley.

INFORMACION RELACIONADA

- Véase la Sentencia del TC 118/2016, de 23 de junio que declara la no inconstitucionalidad del art. 1 de la Ley Orgánica 1/2010, de 19 de febrero. Ref. BOE-A-2010-2739., que añadió la disposición adicional 5, siempre que se interprete en los términos del fundamento jurídico 3 d). Ref. BOE-A-2016-7295.

§ 22

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia

Jefatura del Estado
«BOE» núm. 160, de 6 de julio de 2011
Última modificación: 19 de septiembre de 2020
Referencia: BOE-A-2011-11605

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

Todas las personas tienen derecho a obtener la tutela efectiva de sus derechos ante los tribunales. Así se reconoce en nuestro ordenamiento jurídico en el artículo 24.1 de la Constitución y en el artículo 14.1 del Pacto Internacional de Derechos Civiles y Políticos. Para salvaguardar dichos derechos de los ciudadanos es necesaria la modernización de la Administración de Justicia, campo esencial para consolidar el Estado de Derecho y mejorar la calidad de nuestra democracia. En este contexto de modernización, uno de los elementos de mayor relevancia es, precisamente, la incorporación en las oficinas judiciales de las nuevas tecnologías. Su uso generalizado y obligatorio contribuirá a mejorar la gestión en las oficinas judiciales, actualizando su funcionamiento e incrementando los niveles de eficiencia. Las nuevas tecnologías permiten igualmente abaratar los costes del servicio público de justicia, pero también suponen una mejora de la confianza en el sistema, lo que se traduce en mayor seguridad. Ello incide de manera directa e indirecta en el sistema económico, pues los cambios generan nuevas perspectivas en las relaciones económicas, acrecentando la seguridad y la fluidez de las mismas.

La presente Ley regula el uso de las nuevas tecnologías en la Administración de Justicia. Los principales objetivos de esta norma, son: primero, actualizar el contenido del derecho fundamental a un proceso público sin dilaciones indebidas, gracias a la agilización que permite el uso de las tecnologías en las comunicaciones; segundo, generalizar el uso de las nuevas tecnologías para los profesionales de la justicia; tercero, definir en una norma con rango de ley el conjunto de requisitos mínimos de interconexión, interoperabilidad y seguridad necesarios en el desarrollo de los diferentes aplicativos utilizados por los actores

del mundo judicial, a fin de garantizar la seguridad en la transmisión de los datos y cuantas otras exigencias se contengan en las leyes procesales.

II

En nuestro ordenamiento jurídico existen ya distintos antecedentes que hacían necesaria la aprobación de esta norma.

Así, por un lado, la Ley Orgánica 16/1994, de 8 de noviembre, por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, introdujo, por vez primera en nuestro ordenamiento jurídico, la posibilidad de utilizar medios técnicos, electrónicos e informáticos para el desarrollo de la actividad y el ejercicio de las funciones de juzgados y tribunales. La reforma realizada incluía la posibilidad de dotar a los nuevos documentos o comunicaciones de la validez y eficacia de los originales, siempre que se garantizase la autenticidad, la integridad y el cumplimiento de los requisitos previstos en las leyes procesales.

A partir de esta reforma se han llevado a cabo numerosas modificaciones en distintas normas a fin de hacer efectiva esta previsión. Debe advertirse, eso sí, que estas modificaciones se han producido obedeciendo a necesidades concretas y puntuales detectadas casi siempre en las distintas leyes procesales. También se han aprobado normas relativas a la regulación de aplicaciones y sistemas informáticos utilizados en la Administración de Justicia, así como el establecimiento de registros y sistemas de información y apoyo a la actividad judicial.

El Pleno del Congreso de los Diputados aprobó el día 22 de abril de 2002 una Proposición no de Ley sobre la Carta de Derechos de los Ciudadanos ante la Justicia. Esta Carta señala en su preámbulo que, en los umbrales del siglo XXI, la sociedad española demandaba con urgencia una justicia más abierta que fuese capaz de dar respuesta a los ciudadanos con mayor agilidad, calidad y eficacia, incorporando para ello métodos de organización e instrumentos procesales más modernos y avanzados. Bajo el título «Una Justicia moderna y abierta a los ciudadanos», la primera parte de la Carta recoge los principios que deben inspirar la consecución de dicho objetivo: una justicia transparente y comprensible. El apartado 21, ahondando en la necesidad de que la justicia sea tecnológicamente avanzada, reconoce el derecho «a comunicarse con la Administración de Justicia a través del correo electrónico, videoconferencia y otros medios telemáticos con arreglo a lo dispuesto en las leyes procesales».

Más tarde, la Ley 15/2003, de 26 de mayo, reguladora del régimen retributivo de las carreras judicial y fiscal, consagra el objetivo general de transparencia proclamado en la Carta de Derechos de los Ciudadanos ante la Justicia, creando un instrumento técnico llamado Plan de Transparencia Judicial. Este Plan fue aprobado por Acuerdo de Consejo de Ministros de 21 de octubre de 2005. En él se identifica como instrumento imprescindible para lograr el objetivo de la transparencia la plena utilización de las tecnologías de la información y la comunicación en la Administración de Justicia. Para que este uso sea realidad es necesario unificar o hacer compatibles las distintas aplicaciones informáticas que se utilizan en las oficinas judiciales, así como crear páginas de información en las Administraciones con competencias en materia de justicia. También se declara la necesidad de establecer sistemas adecuados de interconexión y sistemas de intercambio seguro de documentos en los procesos judiciales, así como garantizar la disponibilidad de los sistemas de comunicaciones entre las distintas sedes judiciales electrónicas.

En otro orden de cosas, en 2007 se aprueba la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Esta norma supone el reconocimiento definitivo del derecho de los ciudadanos a comunicarse electrónicamente con las Administraciones públicas. Esta Ley establece el régimen jurídico de la administración electrónica y la gestión electrónica de los procedimientos administrativos y sienta las bases sobre las que debe articularse la cooperación entre las distintas Administraciones para impulsar la administración electrónica.

Por último, en el plano internacional, la Unión Europea ha desarrollado el Plan de Acción E-Justicia. Este Plan de Acción busca la mejora de la eficacia de los sistemas judiciales mediante la aplicación de las tecnologías de información y comunicación en la gestión administrativa de los procesos judiciales. El Plan busca también la cooperación entre las autoridades judiciales y, lo que es más importante, el acceso de los ciudadanos a la justicia.

Para ello, el Plan propone la adopción de medidas coordinadas a nivel nacional y europeo. Su aplicación implicará probablemente modificaciones y adaptaciones en la legislación procesal, así como la creación de un marco regulador de la utilización de las nuevas tecnologías en la Administración de Justicia española, que es el objetivo al que responde esta norma.

III

La Administración de Justicia presenta características que la diferencian de las restantes Administraciones públicas. En primer lugar, por la propia naturaleza de la función que la Administración judicial tiene atribuida, ya que se trata de un poder del Estado distinto del poder ejecutivo, en el que se encuadran las Administraciones públicas que, además, debe satisfacer un derecho fundamental que a su vez es clave para sostener el Estado de Derecho. En segundo lugar, la relación de los ciudadanos con los órganos judiciales se establece casi siempre a través de profesionales, cosa que no suele suceder en el caso de las Administraciones públicas.

Dadas estas características, se ha considerado que la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, no es plenamente aplicable a la Administración de Justicia y es necesaria una regulación específica. Ello no quiere decir, no obstante, que no se hayan adoptado idénticos principios y valores en muchos aspectos.

Así, se ha tenido en cuenta la diferencia entre el procedimiento administrativo y las normas procesales. La presente Ley regula únicamente los aspectos necesarios para dar cumplimiento a la legislación procesal en lo relativo al uso de las nuevas tecnologías. Así, por ejemplo, no se ha buscado establecer plazos o términos distintos de los señalados en las leyes de enjuiciamiento, sino que la norma se limita a establecer los criterios que deben ser considerados para efectuar el cómputo de los mismos si los actos procesales que determinan su comienzo o fin se efectúan a través de medios electrónicos.

También tiene una gran importancia la cooperación entre Administraciones en materia de administración electrónica. Para ello se establecen marcos estables y vinculantes de colaboración, cooperación y coordinación. En este capítulo cobra especial importancia la consolidación como norma legal de algunas de las previsiones contenidas en el Convenio de Colaboración entre el Ministerio de Justicia, el Consejo General del Poder Judicial y la Fiscalía General del Estado para el establecimiento del Esquema judicial de interoperabilidad y seguridad en el ámbito de la Administración de Justicia (EJIS). Asimismo, la Ley crea el Comité técnico estatal de la Administración judicial electrónica, que ostentará competencias en orden a la interoperabilidad de las distintas aplicaciones que se utilizan en la Administración de Justicia, sin perjuicio de las previstas para el Consejo General del Poder Judicial.

IV

La Ley consta de cincuenta y seis artículos agrupados en cinco títulos, doce disposiciones adicionales, dos disposiciones transitorias y cuatro disposiciones finales.

En el Título I se define el objeto de la Ley y su ámbito de aplicación.

El Título II se dedica a regular el uso de medios electrónicos en la Administración de Justicia y se estructura en tres capítulos. El primero de ellos recoge los derechos de los ciudadanos en sus relaciones con dicha Administración, reconociendo la libertad de elección a la hora de establecer tales relaciones y garantizando que la Administración le facilitará los medios necesarios para relacionarse electrónicamente, aún cuando el ciudadano no disponga de los mismos.

El Capítulo II recoge los derechos y deberes de los profesionales del ámbito de la justicia en sus relaciones con la misma por medios electrónicos. Abogados, procuradores, graduados sociales y demás profesionales que actúan en el ámbito de la justicia, además de tener reconocidos los derechos que le son necesarios para el ejercicio de su profesión, utilizarán los medios electrónicos para la presentación de sus escritos y documentos. Esta actividad permitirá la tramitación íntegramente electrónica de los procedimientos judiciales.

El tercer y último Capítulo de este Título recoge la obligación de todos los integrantes de los órganos y oficinas judiciales, así como de las fiscalías, de utilizar exclusivamente los

programas y aplicaciones informáticas puestas a su disposición por las Administraciones competentes.

El Título III aborda el régimen jurídico de la Administración judicial electrónica. En su Capítulo I se define lo que son las sedes judiciales electrónicas y se establece el contenido mínimo de las mismas. A través de dichas sedes se realizarán las actuaciones que lleven a cabo ciudadanos y profesionales con la Administración de Justicia. Se diferencia entre la titularidad de la sede, que viene atribuida a la Administración competente para dotar de medios materiales a los juzgados y tribunales, y el responsable de los contenidos de la misma, que será el órgano que origine la información que se incluya en la sede. Por lo tanto, el titular de una sede será únicamente uno y los responsables tantos como órganos hayan incluido contenidos en la misma. Especial atención merece la posibilidad de crear una o varias sedes electrónicas derivadas o subsedes. Por otro lado, se dispone la creación de un punto de acceso general de la Administración de Justicia, a través del cual se podrá acceder a todas las sedes y subsedes del territorio nacional, con independencia de la posibilidad de acceso directo a las mismas.

El Capítulo II se dedica a las formas de identificación y autenticación, tanto de ciudadanos y profesionales como de la propia Administración de Justicia. Respecto a los primeros, se contempla la posibilidad de uso de diversos sistemas de firma electrónica además del incorporado al Documento Nacional de Identidad. En cuanto a los órganos y oficinas judiciales, se establece la obligatoriedad de que la Administración competente facilite a los mismos los sistemas de firma electrónica consistentes en sello electrónico y código seguro de verificación. Asimismo, en este capítulo se regula el uso de la firma electrónica por parte de todo el personal al servicio de la Administración de Justicia. Por último, se establecen las condiciones para hacer posible la interoperabilidad y autenticación por medio de certificados electrónicos e intercambio electrónico de datos en entornos cerrados de comunicación.

El Título IV fija las condiciones para hacer posible la íntegra tramitación electrónica de los procedimientos judiciales. Dedica el Capítulo II a definir y regular el expediente judicial electrónico, heredero digital de los «autos» que tradicionalmente han constituido el decorado de nuestros juzgados y tribunales. Cuestiones tales como el foliado o la tradicional remisión de los autos, adquieren una dimensión totalmente diferente al amparo de las nuevas tecnologías. Se dispone igualmente qué documentos tienen la consideración de documentos judiciales electrónicos y se aborda una regulación de las copias electrónicas en función del formato del original. Por último, en este capítulo se dedica un artículo a establecer las condiciones en que se deben archivar los documentos judiciales electrónicos.

El Capítulo III de este Título trata del registro de escritos, de las comunicaciones y notificaciones electrónicas. Se establece el principio de que cada oficina judicial con funciones de registro y reparto tendrá asignada una sede electrónica derivada o subsede, de tal forma que cualquier escrito, oficio o comunicación dirigida a un órgano u oficina judicial a los que preste servicio de registro y reparto, deberá tener su entrada a través de dicha subsede electrónica. Se regula el régimen de funcionamiento de dicho registro, así como el cómputo de plazos. Se regula igualmente la forma en que deben comunicarse los ciudadanos y profesionales por medios electrónicos con la Administración de Justicia, así como las condiciones y requisitos que deben cumplir los sistemas que implanten las distintas Administraciones con competencias en las oficinas judiciales para la práctica de actos de comunicación por medios electrónicos.

El Capítulo IV contiene las previsiones relativas a la tramitación electrónica de los procedimientos judiciales. En cuanto al inicio del procedimiento, se establece la obligatoriedad de que el mismo lo sea siempre por medios electrónicos, distinguiendo los casos en que los ciudadanos lo inicien personalmente sin intervención de profesionales, en cuyo caso tendrán a su disposición los medios necesarios para poder hacerlo en dicha forma, de los casos en que comparezcan asistidos por profesionales, en los que serán estos los que tengan la obligación en todo caso de efectuar la presentación del escrito o demanda iniciadora del procedimiento en forma telemática.

Se establecen asimismo las características básicas que deben tener las aplicaciones y sistemas de información utilizados para la gestión por medios electrónicos de los procedimientos judiciales, en orden a garantizar aspectos esenciales de la tramitación

electrónica y la forma en que deben incorporarse a dichos procedimientos los escritos, documentos y otros medios o instrumentos que deban tener acceso a ellos.

Se prevé la forma en que las partes pueden utilizar medios electrónicos para ejercer el derecho reconocido en las leyes procesales a acceder a la información sobre el estado de tramitación de los procedimientos.

El Título V de la Ley aborda los aspectos básicos sobre los que debe asentarse la necesaria cooperación y colegiación de esfuerzos entre las Administraciones con competencias en materia de justicia. Se constituye el Comité técnico estatal de la Administración judicial electrónica con importantes competencias en orden a favorecer la compatibilidad y a asegurar la interoperabilidad de los sistemas y aplicaciones empleados en la Administración de Justicia, así como para asegurar la cooperación entre las distintas Administraciones.

Se define el contenido del Esquema judicial de interoperabilidad y seguridad, al considerarse dichas cualidades como esenciales para un eficaz y eficiente funcionamiento del sistema, estableciéndose que deberá tenerse presente y acomodarse al mismo todos los servicios, sistemas y aplicaciones utilizados en la Administración de Justicia a lo largo de su ciclo de vida.

Se establecen los principios generales a los que deberán responder tanto la interoperabilidad entre las distintas aplicaciones como la seguridad de la información contenida en ellas.

Como concreción del principio de cooperación al que obedece la presente Ley, se dispone la posibilidad de la reutilización de sistemas, infraestructuras y aplicaciones de las Administraciones con competencias en materia de justicia.

Por último, en las disposiciones adicionales se establecen los plazos a los que se deben ajustar las distintas Administraciones con competencias en materia de justicia para el íntegro establecimiento en las oficinas judiciales y fiscalías de los medios e instrumentos necesarios para la efectiva implantación de las tecnologías de la información y comunicación.

TÍTULO I

Del ámbito de aplicación y los principios generales

Artículo 1. *Objeto.*

1. La presente Ley regula la utilización de las tecnologías de la información por parte de los ciudadanos y profesionales en sus relaciones con la Administración de Justicia y en las relaciones de la Administración de Justicia con el resto de Administraciones y organismos públicos, en los términos recogidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

2. En la Administración de Justicia se utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando el acceso, la autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones.

Artículo 2. *Ámbito de aplicación.*

La presente Ley será de aplicación a la Administración de Justicia, a los ciudadanos en sus relaciones con ella y a los profesionales que actúen en su ámbito, así como a las relaciones entre aquélla y el resto de Administraciones y organismos públicos.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley, los términos relacionados en el anexo tendrán el significado que resulta de las definiciones contenidas en el mismo.

TÍTULO II

Uso de los medios electrónicos en la Administración de Justicia

CAPÍTULO I

Derechos de los ciudadanos en sus relaciones con la Administración de Justicia por medios electrónicos

Artículo 4. *Derechos de los ciudadanos.*

1. Los ciudadanos tienen derecho a relacionarse con la Administración de Justicia utilizando medios electrónicos para el ejercicio de los derechos previstos en los Capítulos I y VII del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la forma y con las limitaciones que en los mismos se establecen.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad judicial, y en los términos previstos en la presente Ley, los siguientes derechos:

a) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con la Administración de Justicia.

b) A la igualdad en el acceso electrónico a los servicios de la Administración de Justicia.

c) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean parte procesal legítima, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

d) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de parte o acrediten interés legítimo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

e) A la conservación en formato electrónico por la Administración de Justicia de los documentos electrónicos que formen parte de un expediente conforme a la normativa vigente en materia de archivos judiciales.

f) A utilizar los sistemas de identificación y firma establecidos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

g) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

h) A la calidad de los servicios públicos prestados por medios electrónicos.

i) A elegir las aplicaciones o sistemas para relacionarse con la Administración de Justicia siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos y, en todo caso, siempre que sean compatibles con los que dispongan los juzgados y tribunales y se respeten las garantías y requisitos previstos en el procedimiento que se trate.

Artículo 5. *Prestación de servicios y disposición de medios e instrumentos electrónicos.*

1. Las Administraciones con competencia en materia de justicia habilitarán diferentes canales o medios para la prestación de los servicios electrónicos, asegurando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.

2. Las Administraciones competentes en materia de justicia asegurarán el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:

a) Las oficinas de información y atención al público, en los procedimientos en los que los ciudadanos comparezcan y actúen sin asistencia letrada y sin representación procesal, pondrán a su disposición de forma libre y gratuita los medios e instrumentos precisos para

ejercer los derechos reconocidos en el artículo 4 de esta Ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

b) Puntos de acceso electrónico, consistentes en sedes judiciales electrónicas creadas y gestionadas por las distintas Administraciones competentes en materia de justicia y disponibles para los ciudadanos a través de redes de comunicación, para sus relaciones con la Administración de Justicia.

c) Las Administraciones con competencias en materia de justicia publicarán la relación de todos los puntos de acceso electrónico.

d) Servicios de atención telefónica con los criterios de seguridad y las posibilidades técnicas existentes, que faciliten a los ciudadanos las relaciones con la Administración de Justicia en lo que se refiere a los servicios electrónicos mencionados en los apartados anteriores.

e) Puntos de información electrónicos, ubicados en los edificios judiciales.

CAPÍTULO II

Derechos y deberes de los profesionales de la justicia en sus relaciones con la Administración de Justicia por medios electrónicos

Artículo 6. *Derechos y deberes de los profesionales del ámbito de la justicia.*

1. Los profesionales de la justicia tienen el derecho a relacionarse con la misma a través de medios electrónicos.

2. Además, los profesionales tienen, en relación con la utilización de los medios electrónicos en la actividad judicial y en los términos previstos en la presente Ley, los siguientes derechos:

a) A acceder y conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean representantes procesales de la parte personada, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

b) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que sean representantes procesales de la parte personada o acrediten interés legítimo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

c) A la conservación en formato electrónico por la Administración de Justicia de los documentos electrónicos que formen parte de un expediente según la normativa vigente en materia de archivos judiciales.

d) A utilizar los sistemas de identificación y firma establecidos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, siempre que dicho sistema le identifique de forma unívoca como profesional para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales.

A tal efecto, el Consejo General o el superior correspondiente deberá poner a disposición de las oficinas judiciales los protocolos y sistemas de interconexión que permitan el acceso necesario por medios electrónicos al registro de profesionales colegiados ejercientes previsto en el artículo 10 de la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, garantizando que en él consten sus datos profesionales, tales como número de colegiado, domicilio profesional, número de teléfono y dirección de correo electrónico.

e) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

3. Los profesionales de la justicia, en los términos previstos en la presente Ley, tienen el deber de utilizar los medios electrónicos, las aplicaciones o los sistemas establecidos por las

Administraciones competentes en materia de justicia, respetando en todo caso las garantías y requisitos previstos en el procedimiento que se trate.

Artículo 7. *Prestación de servicios y disposición de medios e instrumentos electrónicos.*

Las Administraciones competentes en materia de justicia asegurarán el acceso de los profesionales a los servicios electrónicos proporcionados en su ámbito a través de puntos de acceso electrónico, consistentes en sedes judiciales electrónicas creadas y gestionadas por aquéllas y disponibles para los profesionales a través de redes de comunicación, para sus relaciones con la Administración de Justicia, en los términos previstos en la presente Ley.

CAPÍTULO III

Utilización obligatoria de los medios electrónicos en la tramitación de los procedimientos electrónicos judiciales

Artículo 8. *Uso obligatorio de medios e instrumentos electrónicos.*

Los sistemas informáticos puestos al servicio de la Administración de Justicia serán de uso obligatorio en el desarrollo de la actividad de los órganos y oficinas judiciales y de las fiscalías por parte de todos los integrantes de las mismas, conforme a los criterios e instrucciones de uso que dicten, en el ámbito de sus competencias, el Consejo General del Poder Judicial, la Fiscalía General del Estado y las Administraciones competentes, así como a los protocolos de actuación aprobados por los Secretarios de Gobierno.

Las Administraciones competentes proporcionarán los medios seguros para que estos sistemas sean plenamente accesibles y operativos sin necesidad de que los usuarios se encuentren físicamente en las sedes de sus respectivos órganos, oficinas o fiscalías.

TÍTULO III

Régimen jurídico de la Administración judicial electrónica

CAPÍTULO I

De la sede judicial electrónica

Artículo 9. *Sede judicial electrónica.*

1. La sede judicial electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a cada una de las Administraciones competentes en materia de justicia.

2. Las sedes judiciales electrónicas se crearán mediante disposición publicada en el «Boletín Oficial del Estado» o el «Boletín Oficial de la Comunidad Autónoma» correspondiente, y tendrán, al menos, los siguientes contenidos:

a) Identificación de la dirección electrónica de referencia de la sede que incluya el nombre del dominio que le otorgue la Administración competente.

b) Identificación de su titular, así como del órgano u órganos administrativos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos y profesionales en la misma.

c) Identificación de los canales de acceso a los servicios disponibles en la sede, con expresión, en su caso, de los teléfonos y oficinas a través de los cuales también puede accederse a los mismos.

d) Cauces disponibles para la formulación de sugerencias y quejas con respecto al servicio que presta la sede.

3. El establecimiento de una sede judicial electrónica conlleva la responsabilidad del titular de garantizar la integridad y actualización de la información facilitada, así como el acceso a los servicios previstos en la misma.

4. Las Administraciones competentes en materia de justicia determinarán las condiciones e instrumentos de creación de las sedes judiciales electrónicas, con sujeción a los principios de publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.

5. La publicación en las sedes judiciales electrónicas de informaciones, servicios y transacciones respetará los estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

Artículo 10. *Características de las sedes judiciales electrónicas y sus clases.*

1. Se realizarán a través de sedes judiciales electrónicas todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración de Justicia o de los ciudadanos y profesionales por medios electrónicos.

2. Las sedes judiciales electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

3. Se podrán crear una o varias sedes judiciales electrónicas derivadas de una sede judicial electrónica. Las sedes judiciales electrónicas derivadas, o subsedes, deberán resultar accesibles desde la dirección electrónica de la sede principal, sin perjuicio de que sea posible el acceso electrónico directo.

4. La Administración competente creará una sede judicial electrónica derivada para cada uno de los servicios de recepción de escritos, registro y reparto de asuntos existentes, en función de su organización y cuyos contenidos serán gestionados por el propio servicio. En el caso de que exista un único servicio de recepción de escritos, registro y reparto, la sede judicial electrónica asumirá las funciones de las subsedes.

5. Igualmente la Administración competente creará una sede judicial electrónica derivada en cada una de las oficinas fiscales que tengan servicio de registro y reparto.

6. Las sedes judiciales electrónicas derivadas se crearán por disposición del órgano administrativo que tenga atribuida esta competencia y deberán cumplir los mismos requisitos de publicidad que las sedes judiciales electrónicas principales. Cuando los servicios de recepción de escritos, registro y reparto de asuntos no sean creados con una sede o subsede judicial electrónica, deberán recibir la misma publicidad que éstas.

Artículo 11. *Contenido y servicios de las sedes judiciales electrónicas.*

1. Toda sede judicial electrónica dispondrá, al menos, de los siguientes contenidos:

a) Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión, de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

b) Información necesaria para su correcta utilización, incluyendo el mapa de la sede judicial electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles.

c) Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.

d) Relación de sistemas de firma electrónica que, conforme a lo previsto en esta Ley, sean admitidos o utilizados en la sede.

e) Normas de creación del registro o registros electrónicos accesibles desde la sede.

f) Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos y las de las Agencias Autonómicas de Protección de Datos.

2. Las sedes judiciales electrónicas dispondrán, al menos, de los siguientes servicios a disposición de los ciudadanos y profesionales:

a) La relación de los servicios disponibles en la sede judicial electrónica.

b) La carta de servicios y la carta de servicios electrónicos.

c) La relación de los medios electrónicos que los ciudadanos y profesionales pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con la Administración de Justicia.

d) Un enlace para la formulación de sugerencias y quejas ante los órganos correspondientes.

e) Acceso, en los términos legalmente establecidos, al estado de tramitación del expediente.

f) Un enlace al Tablón Edictal Judicial único, como medio de publicación y consulta de las resoluciones y comunicaciones que por disposición legal deban fijarse en el tablón de anuncios o edictos.

g) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

h) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

i) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.

j) La Carta de Derechos de los Ciudadanos ante la Justicia.

3. No será necesario recoger en las subsedes la información y los servicios a que se refieren los apartados anteriores cuando ya figuren en la sede de la que aquéllas derivan.

4. La sede judicial electrónica garantizará el régimen de cooficialidad lingüística vigente en su territorio.

Artículo 12. *Reglas especiales de responsabilidad.*

1. El órgano que origine la información que se deba incluir en la sede judicial electrónica, será el responsable de la veracidad e integridad de su contenido.

2. La sede judicial electrónica establecerá los medios necesarios para que el ciudadano conozca si la información o servicio al que accede corresponde a la propia sede o a un punto de acceso que no tiene el carácter de sede o a un tercero.

Artículo 13. *Punto de acceso general de la Administración de Justicia.*

1. El punto de acceso general de la Administración de Justicia contendrá el directorio de las sedes judiciales electrónicas que, en este ámbito, faciliten el acceso a los servicios, procedimientos e informaciones accesibles correspondientes a la Administración de Justicia, al Consejo General del Poder Judicial, a la Fiscalía General del Estado y a los organismos públicos vinculados o dependientes de la misma, así como a las Administraciones con competencias en materia de justicia. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras Administraciones públicas o corporaciones que representen los intereses de los profesionales de la justicia, mediante la celebración de los correspondientes convenios.

2. El punto de acceso general será creado y gestionado por el Ministerio de Justicia conforme a los acuerdos que se adopten en el Comité técnico estatal de la Administración judicial electrónica, para asegurar la completa y exacta incorporación de la información y accesos publicados en éste.

CAPÍTULO II

De la identificación y autenticación

Sección 1.ª Disposiciones comunes

Artículo 14. *Formas de identificación y autenticación.*

1. La Administración de Justicia admitirá, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y resulten adecuados para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Sin perjuicio de lo dispuesto en los artículos 4 y 6 de la presente Ley y en todo caso, con sujeción estricta a lo dispuesto por las leyes procesales, los ciudadanos y profesionales

del ámbito de la Justicia podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con la Administración de Justicia:

a) Los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.
b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones públicas.
c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

3. La Administración de Justicia podrá utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzca:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede judicial electrónica y el establecimiento con ella de comunicaciones seguras.
b) Sistemas de firma electrónica para la actuación judicial automatizada.
c) Firma electrónica del personal al servicio de la Administración de Justicia.
d) Sistemas de intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo que específicamente se haya convenido.

Artículo 15. *Identificación de las personas jurídicas y entidades sin personalidad jurídica y autenticación de su actuación.*

Las personas jurídicas y entidades sin personalidad jurídica podrán utilizar sistemas de firma electrónica de persona jurídica o de entidades sin personalidad jurídica para todos aquellos procedimientos y actuaciones ante la Administración de Justicia en los términos establecidos en las leyes procesales.

Artículo 16. *Régimen de uso de la firma electrónica.*

1. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean necesarios de acuerdo con la legislación aplicable.
2. Los órganos de la Administración de Justicia u organismos públicos vinculados o dependientes podrán tratar los datos personales consignados, a los solos efectos de la verificación de la firma.

Artículo 17. *Régimen de sustitución y habilitación entre profesionales.*

El régimen de acceso a los servicios electrónicos en el ámbito de la Administración de Justicia para los supuestos de sustitución entre profesionales, así como para la habilitación de sus empleados, se regulará por la respectiva Administración competente mediante disposiciones reglamentarias.

Sección 2.ª Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia

Artículo 18. *Identificación de las sedes judiciales electrónicas.*

1. Las sedes judiciales electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.
2. Las direcciones electrónicas de la Administración de Justicia y de los organismos públicos vinculados o dependientes de la misma que tengan la condición de sedes judiciales electrónicas deberán hacerlo constar de forma visible e inequívoca.

3. El instrumento de creación de la sede judicial electrónica será accesible directamente o mediante enlace a su publicación en el «Boletín Oficial del Estado» o en el de la Comunidad Autónoma correspondiente.

4. Los sistemas de información que soporten las sedes judiciales electrónicas deberán asegurar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. El Esquema judicial de interoperabilidad y seguridad establecerá las previsiones necesarias para ello, en el marco de la colaboración entre el Consejo General del Poder Judicial, el Ministerio de Justicia, la Fiscalía General del Estado y las Comunidades Autónomas con competencias en materia de justicia.

Artículo 19. *Sistemas de firma electrónica para la actuación judicial automatizada.*

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación judicial automatizada, la Administración competente facilitará a cada una de las oficinas judiciales del ámbito de su competencia los siguientes sistemas de firma electrónica:

a) Sello electrónico de la oficina judicial basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a cada oficina judicial, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede judicial electrónica correspondiente.

2. Los certificados electrónicos a los que se hace referencia en la letra a) del apartado 1 incluirán la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de oficina judicial.

3. La relación de sellos electrónicos utilizados por la Administración de Justicia, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración competente adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

Artículo 20. *Sistemas de firma electrónica mediante sello electrónico.*

1. La creación de sellos electrónicos se realizará mediante resolución de la autoridad competente, que se publicará en la sede judicial electrónica correspondiente y en la que deberá constar:

a) Organismo u órgano titular del sello, que será el responsable de su utilización, con indicación de su adscripción en la Administración de Justicia u organismo público dependiente de la misma.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y documentos en los que podrá ser utilizado.

2. Los certificados de sello electrónico tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».

b) Nombre del suscriptor.

c) Número de identificación judicial.

3. El modo de emitir los certificados electrónicos de sello electrónico y sus contenidos se definirán en el Esquema judicial de interoperabilidad y seguridad.

Artículo 21. *Firma electrónica de magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la Administración de Justicia y otros entes públicos.*

1. Sin perjuicio de lo previsto en los artículos 9 y 10 sobre la sede judicial electrónica, la identificación y autenticación del ejercicio de la competencia de la oficina judicial actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, de acuerdo con lo dispuesto en los siguientes apartados.

2. Las Administraciones, en el ámbito de sus competencias, proveerán a secretarios judiciales, fiscales, forenses y demás personal al servicio de la Administración de Justicia, de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo y el cargo e identificar también a la oficina u órgano judicial en la que presta sus servicios.

El Ministerio de Justicia facilitará a las Administraciones competentes datos actualizados de los fiscales y secretarios judiciales a fin de dotarles de firma electrónica.

3. Los sistemas de firma electrónica de jueces y magistrados serán los que provea el Consejo General del Poder Judicial. Este podrá establecer, a través de convenios, que el proveedor sea la Administración competente.

4. Las Administraciones, en el ámbito de sus competencias, dotarán de sistemas de firma electrónica a los representantes procesales del Estado y demás entes públicos, a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Sección 3.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos

Artículo 22. *Interoperabilidad de la identificación y autenticación por medio de certificados electrónicos.*

1. Los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por la Administración de Justicia como válidos en las relaciones con la misma, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones competentes en materia de justicia la información que se precise en condiciones que resulten tecnológicamente viables, bajo principios de reconocimiento mutuo y reciprocidad y sin que suponga coste alguno para aquéllas.

2. Las Administraciones competentes dispondrán de acceso, al menos, a alguna plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de la Administración de Justicia, que será de libre acceso por parte de todos los órganos judiciales.

Artículo 23. *Identificación y autenticación de los ciudadanos por funcionario público.*

1. En los supuestos en que para la realización de cualquier actuación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 14 de los que aquél no disponga, tal identificación o autenticación será válidamente realizada por un funcionario mediante el uso del sistema de firma electrónica del que esté dotado.

2. Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

Artículo 24. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones con competencias en materia de justicia, órganos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el presente artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a la Administración de Justicia, el Comité técnico estatal de la Administración judicial electrónica determinará las condiciones y garantías por las que se regirán, que al menos comprenderán la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones o a entidades de derecho público, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

TÍTULO IV

De la tramitación electrónica de los procedimientos judiciales

CAPÍTULO I

Disposiciones comunes

Artículo 25. *Criterios para la gestión electrónica.*

1. La gestión electrónica de la actividad judicial respetará el cumplimiento de los requisitos formales y materiales establecidos en las normas procesales. A estos efectos se impulsará la aplicación de medios electrónicos a los procesos de trabajo y a la gestión de los procedimientos y de la actuación judicial.

2. La aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización por el Comité técnico estatal de la Administración judicial electrónica de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio, en el que se considerarán especialmente los siguientes aspectos:

a) La posible supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones.

b) La reducción de los tiempos en la tramitación de los procedimientos.

c) La racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas y la introducción de indicadores de gestión.

CAPÍTULO II

Del expediente judicial electrónico

Artículo 26. *Expediente judicial electrónico.*

1. El expediente judicial electrónico es el conjunto de datos, documentos, trámites y actuaciones electrónicas, así como de grabaciones audiovisuales correspondientes a un procedimiento judicial, cualquiera que sea el tipo de información que contenga y el formato en el que se hayan generado.

2. Se asignará un número de identificación general a aquellos documentos que puedan generar un nuevo procedimiento, que será único e inalterable a lo largo de todo el proceso, permitiendo su identificación unívoca por cualquier órgano del ámbito judicial en un entorno de intercambio de datos.

3. El foliado de los expedientes judiciales electrónicos se llevará a cabo mediante un índice electrónico, firmado por la oficina judicial actuante, según proceda. Este índice garantizará la integridad del expediente judicial electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes judiciales electrónicos.

4. La remisión de expedientes se sustituirá a todos los efectos legales por la puesta a disposición del expediente judicial electrónico, teniendo derecho a obtener copia electrónica del mismo todos aquellos que lo tengan conforme a lo dispuesto en las normas procesales.

Artículo 27. *Documento judicial electrónico.*

1. Tendrán la consideración de documentos judiciales electrónicos las resoluciones y actuaciones que se generen en los sistemas de gestión procesal, así como toda información que tenga acceso de otra forma al expediente, cuando incorporen datos firmados electrónicamente en la forma prevista en la Sección 2.ª del Capítulo II del Título III de la presente Ley.

2. Las Administraciones competentes, en su relación de prestadores de servicios de certificación electrónica, especificarán aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

3. Tendrá la consideración de documento público el documento electrónico que incluya la fecha electrónica y que incorpore la firma electrónica reconocida del secretario judicial, siempre que actúe en el ámbito de sus competencias, conforme a lo dispuesto en las leyes procesales.

Artículo 28. *Copias electrónicas.*

1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las oficinas judiciales, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en las leyes procesales, siempre que el documento electrónico original se encuentre en poder de la oficina judicial donde haya sido originado o incorporado y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

Si se alterase el formato original, deberá incluirse en los metadatos la condición de copia.

2. Las copias realizadas por las oficinas judiciales, utilizando medios electrónicos, de documentos emitidos originalmente por ellas en soporte papel tendrán la consideración de copias auténticas.

3. Las oficinas judiciales podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

4. A los documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, se les dará el destino previsto en la normativa vigente en materia de archivos judiciales.

5. Las copias realizadas en soporte papel de documentos judiciales electrónicos y firmados electrónicamente por el secretario judicial tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código seguro de verificación que permita contrastar su autenticidad mediante el acceso a los archivos electrónicos de la oficina judicial emisora.

Artículo 29. *Archivo electrónico de documentos.*

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones judiciales.

Los Archivos Judiciales de Gestión, Territoriales y Central serán gestionados mediante programas y aplicaciones informáticas, compatibles con los ya existentes en juzgados y tribunales, adaptados a las funciones y cometidos de cada uno, cuyo funcionamiento electrónico será regulado mediante Real Decreto.

2. Los documentos electrónicos que contengan actos procesales que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados y ajustarse a los requerimientos que garanticen la compatibilidad e interoperabilidad de los sistemas informáticos. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como lo previsto en los artículos 234 y 235 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

4. Sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, el Consejo General del Poder Judicial regulará reglamentariamente la reutilización de sentencias y otras resoluciones judiciales por medios

digitales de referencia o reenvío de información, sea o no con fines comerciales, por parte de personas físicas o jurídicas para facilitar el acceso a las mismas de terceras personas.

CAPÍTULO III

Del registro de escritos, las comunicaciones y las notificaciones electrónicas

Sección 1.ª Del registro de escritos

Artículo 30. *Registro judicial electrónico.*

1. Las Administraciones competentes dotarán a las oficinas judiciales con funciones de registro de los medios electrónicos adecuados para la recepción y registro de escritos y documentos, traslado de copias, realización de actos de comunicación y expedición de resguardos electrónicos a través de medios de transmisión seguros, entre los que se incluirán los sistemas de firma y sellado de tiempo electrónicos reconocidos.

2. Los registros judiciales electrónicos creados en las condiciones del apartado anterior se corresponderán con la subsede judicial electrónica.

3. En estos registros judiciales electrónicos únicamente se admitirán escritos y documentos dirigidos a las oficinas judiciales dependientes del mismo, conforme a lo establecido en el artículo 230 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y en las leyes procesales.

4. La recepción de solicitudes, escritos y comunicaciones podrá interrumpirse por el tiempo imprescindible sólo cuando concurran razones justificadas de mantenimiento técnico u operativo. La interrupción deberá anunciarse a los potenciales usuarios del registro electrónico con la antelación que, en cada caso, resulte posible.

En supuestos de interrupción no planificada en el funcionamiento del registro electrónico, y siempre que sea posible, se dispondrán las medidas para que el usuario resulte informado de esta circunstancia, así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. Alternativamente, podrá establecerse un redireccionamiento que permita utilizar un registro electrónico en sustitución de aquél en el que se haya producido la interrupción.

Artículo 31. *Funcionamiento.*

1. Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, documento o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

2. Los documentos que se acompañen al correspondiente escrito o comunicación, deberán cumplir los estándares de formato y requisitos de seguridad que se determinen en el marco institucional de cooperación en materia de administración electrónica. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados, así como la fecha y hora de presentación y el número de registro de entrada en la correspondiente sede judicial electrónica.

Artículo 32. *Cómputo de plazos.*

1. Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las oficinas judiciales por la fecha y hora oficial de la sede judicial electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.

2. Los registros electrónicos permitirán la presentación de escritos, documentos y comunicaciones todos los días del año durante las veinticuatro horas.

3. A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación, en un día inhábil a efectos procesales conforme a la ley, se entenderá realizada en la primera hora del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

4. El inicio del cómputo de los plazos que hayan de cumplir las oficinas judiciales vendrá determinado por la fecha y hora de presentación en el propio registro.

5. Cada sede judicial electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquélla, los días que se considerarán inhábiles a los efectos de los apartados anteriores.

Artículo 32 bis. *Archivos electrónicos de apoderamientos apud acta.*

1. Asimismo, se dispondrá en las oficinas judiciales con funciones de registro, de un archivo electrónico de apoderamientos en el que deberán inscribirse los apoderamientos apud acta otorgados presencial o electrónicamente por quien ostente la condición de interesado en un procedimiento judicial a favor de representante, para actuar en su nombre ante la Administración de Justicia.

Ello no impedirá la existencia de archivos electrónicos de apoderamientos apud acta en cada oficina judicial para la realización de los trámites específicos en cada una.

2. Los archivos electrónicos de apoderamientos apud acta deberán ser plenamente interoperables entre sí, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se registren en sus correspondientes archivos.

Los archivos electrónicos de apoderamientos apud acta permitirán comprobar válidamente la representación que ostentan quienes actúen ante la Administración de Justicia en nombre de un tercero.

3. Los asientos que se realicen en los archivos electrónicos de apoderamientos apud acta deberán contener, al menos, la siguiente información:

a) Nombre y apellidos o razón social, número de documento nacional de identidad, de identificación fiscal o de documento equivalente del poderdante.

b) Nombre y apellidos o razón social, número de documento nacional de identidad, de identificación fiscal o de documento equivalente del apoderado.

c) Fecha de inscripción.

d) Tipo de poder según las facultades que otorgue.

4. Los apoderamientos apud acta que se inscriban en los archivos electrónicos de apoderamientos apud acta deberán corresponder a alguna de las siguientes tipologías:

a) Un poder general para que el apoderado pueda actuar en nombre del poderdante en cualquier actuación judicial.

b) Un poder para que el apoderado pueda actuar en nombre del poderdante únicamente en determinadas clases de procedimientos.

c) Un poder especial para que el apoderado pueda actuar en nombre del poderdante en un procedimiento concreto.

5. El poder inscribible en que la parte otorgue su representación al apoderado habrá de ser conferido por comparecencia apud acta.

El apoderamiento apud acta se otorgará mediante comparecencia electrónica en la correspondiente sede electrónica judicial haciendo uso de los sistemas de firma electrónica previstos en esta Ley, o bien mediante comparecencia personal ante el secretario judicial de cualquier oficina judicial.

6. Los apoderamientos inscritos en el archivo tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción. En todo caso, en cualquier momento antes de la finalización de dicho plazo el poderdante podrá revocar o prorrogar el poder. Las prórrogas otorgadas por el poderdante al apoderamiento tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción.

7. Las solicitudes de revocación, de prórroga o de denuncia del mismo podrán dirigirse a cualquier archivo, debiendo quedar inscrita esta circunstancia en el archivo ante el que tenga efectos el poder y surtiendo efectos desde la fecha en la que se produzca dicha inscripción.

Sección 2.ª De las comunicaciones y las notificaciones electrónicas

Artículo 33. *Comunicaciones electrónicas.*

1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con la Administración de Justicia, sea o no por medios electrónicos.

Asimismo, se podrá establecer legal o reglamentariamente la obligatoriedad de comunicarse con ella utilizando solo medios electrónicos cuando se trate de personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

2. Las comunicaciones a través de medios electrónicos se realizarán, en todo caso, con sujeción a lo dispuesto en la legislación procesal y serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones, y se identifique con la autenticación que sea exigible al remitente y al destinatario de las mismas.

3. Las Administraciones competentes en materia de justicia publicarán, en el correspondiente «Diario Oficial» y en la propia sede judicial electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con las oficinas judiciales.

4. Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal y en las leyes procesales.

5. Los profesionales de la justicia deberán realizar sus comunicaciones por medios electrónicos cuando técnicamente estén disponibles.

6. Las oficinas judiciales utilizarán en todo caso medios electrónicos en sus comunicaciones con otras Administraciones y organismos públicos, salvo imposibilidad legal o material.

Artículo 34. *Práctica de actos de comunicación por medios electrónicos.*

1. El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la salida y las de la puesta a disposición del interesado del acto objeto de notificación, así como de acceso a su contenido.

2. En caso de que el acto de comunicación no pueda llevarse a cabo por medios electrónicos, se procederá a imprimir la resolución y la documentación necesaria, procediéndose a la práctica del acto de comunicación en la forma establecida en las leyes procesales e incorporándose a continuación el documento acreditativo de la práctica del acto de comunicación, debidamente digitalizado, al expediente judicial electrónico. En todo caso, el destinatario del acto de comunicación tendrá derecho a obtener copia de la documentación recibida en formato electrónico.

Artículo 35. *Comunicación edictal electrónica.*

La publicación de resoluciones y comunicaciones que por disposición legal deban fijarse en tablón de anuncios, así como la publicación de los actos de comunicación procesal que deban ser objeto de inserción en el «Boletín Oficial del Estado», en el de la Comunidad Autónoma o en el de la provincia respectiva, serán sustituidas en todos los órdenes jurisdiccionales por su publicación en el Tablón Edictal Judicial único previsto en el artículo 236 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

El Tablón Edictal Judicial Único será publicado electrónicamente por la Agencia Estatal Boletín Oficial del Estado, en la forma en que se disponga reglamentariamente. A tal efecto, la Agencia Estatal Boletín Oficial del Estado pondrá a disposición de los juzgados y tribunales un sistema automatizado de remisión y gestión telemática que garantizará la celeridad en la publicación de los edictos, su correcta y fiel inserción, así como la identificación del órgano remitente.

CAPÍTULO IV

De la tramitación electrónica

Artículo 36. *Iniciación del procedimiento por medios electrónicos.*

1. La iniciación de un procedimiento judicial por medios electrónicos por los ciudadanos, en aquellos juicios en los que pueden comparecer de forma personal y directa por no ser preceptiva la asistencia letrada ni la representación por procurador conforme a lo establecido en las normas de procedimiento, requerirá la puesta a disposición de los interesados de los correspondientes modelos o impresos normalizados en la sede judicial electrónica, que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

2. En todo caso, cuando los escritos fueran presentados en papel por las personas a las que se refiere el apartado primero del presente artículo, se procederá a su digitalización por la sección correspondiente del servicio común procesal que tenga atribuidas dichas funciones.

3. Los profesionales de la justicia presentarán sus demandas y otros escritos por vía telemática a través de los sistemas previstos en esta Ley, empleando firma electrónica reconocida.

4. Todo escrito iniciador del procedimiento deberá ir acompañado de un formulario normalizado debidamente cumplimentado en los términos que se establezcan reglamentariamente.

Artículo 37. *Tramitación del procedimiento utilizando medios electrónicos.*

1. Las aplicaciones y sistemas de información utilizados para la gestión por medios electrónicos de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación del órgano u oficina responsable de los procedimientos, así como la tramitación ordenada de los expedientes, y facilitar la simplificación y la publicidad de los procedimientos.

2. Los sistemas de comunicación utilizados en la gestión electrónica de los procedimientos para las comunicaciones entre las unidades intervinientes en la tramitación de las distintas fases del proceso deberán cumplir los requisitos establecidos en esta Ley y en las disposiciones reglamentarias de desarrollo.

3. Cuando se utilicen medios electrónicos en la gestión del procedimiento, los actos de comunicación y notificación que hayan de practicarse se realizarán conforme a las disposiciones contenidas en los artículos 33 a 35 de esta Ley.

4. Los expedientes y demás actuaciones que deban ser remitidos por otras Administraciones y organismos públicos deberán realizarse en todo caso por vía telemática a través de la correspondiente sede judicial electrónica. El expediente administrativo electrónico habrá de cumplir los requisitos previstos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, y deberá remitirse debidamente foliado mediante un índice electrónico que permita la debida localización y consulta de los documentos incorporados.

Artículo 38. *Presentación de escritos, documentos u otros medios o instrumentos.*

1. La presentación de toda clase de escritos, documentos, dictámenes, informes u otros medios o instrumentos se ajustará a lo dispuesto en las leyes procesales, debiendo ir acompañados en todo caso del formulario normalizado a que se refiere el apartado 4 del artículo 36, en el que además se consignará el tipo y número de expediente y año al que se refiera el escrito.

2. En todo caso, la presentación de escritos, documentos y otros medios o instrumentos se ajustará a las siguientes reglas:

a) Los documentos en papel que, conforme a lo dispuesto en las leyes procesales puedan o deban ser aportados por las partes en cualquier momento del procedimiento, deberán ser incorporados como anexo al documento principal mediante imagen digitalizada

de la copia, si fueran públicos, o del original del documento obrante en papel, si se tratara de documentos privados. El archivo de la imagen digitalizada habrá de ir firmado mediante la utilización de los sistemas de firma electrónica previstos en la presente Ley, en las leyes procesales o en otras normas de desarrollo.

b) Los documentos electrónicos públicos o privados se incorporarán como anexo al documento principal siguiendo los sistemas previstos en esta Ley o en sus normas de desarrollo y conforme a lo previsto en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

c) En caso de que fueran impugnados por la parte contraria, se procederá conforme a lo dispuesto en las leyes procesales y, en su caso, en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

d) No se admitirá la aportación en otra forma, salvo en el supuesto de que, por las singularidades características del documento, el sistema no permita su incorporación como anexo para su envío por vía telemática. En estos casos, el usuario hará llegar dicha documentación al destinatario por otros medios en la forma que establezcan las normas procesales, y deberá hacer referencia a los datos identificativos del envío telemático al que no pudo ser adjuntada, presentando el original ante el órgano judicial en el día siguiente hábil a aquel en que se hubiera efectuado el envío telemático. Tales documentos serán depositados y custodiados por quien corresponda en el archivo, de gestión o definitivo, de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia únicamente en formato papel.

Cuando se deban incorporar documentos sobre los cuales existan sospechas de falsedad, deberá aportarse en todo caso además el documento original, al que se le dará el tratamiento contemplado en el párrafo anterior.

e) En los casos en que se deban aportar al procedimiento medios o instrumentos de prueba que por su propia naturaleza no sean susceptibles de digitalización, serán depositados y custodiados por quien corresponda en el archivo de gestión o definitivo de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia.

Artículo 39. *Traslado de copias.*

El traslado de copias por vía telemática se realizará de forma simultánea a la presentación telemática de escritos y documentos ante el órgano u oficina judicial correspondiente.

Artículo 40. *Acreditación de la representación procesal.*

1. Se aportará copia electrónica del poder notarial de representación conferido al procurador. En caso de impugnación, el secretario judicial procederá a comprobar el apoderamiento a través de la Agencia Notarial de Certificación.

2. La representación otorgada por comparecencia apud-acta ante secretario judicial se acreditará adjuntando copia electrónica de la misma o mediante indicación del número, fecha y secretario judicial ante quien se otorgó.

3. El apoderamiento podrá igualmente acreditarse mediante la certificación de su inscripción en el archivo electrónico de apoderamientos apud acta de las oficinas judiciales.

Artículo 41. *Acceso de las partes a la información sobre el estado de tramitación.*

Se pondrá a disposición de las partes un servicio electrónico de acceso restringido donde éstas puedan consultar, previa identificación y autenticación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información y con pleno respeto a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y legislación que la desarrolla. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados.

Artículo 42. *Actuación judicial automatizada.*

En caso de actuación automatizada, deberá establecerse previamente por el Comité técnico estatal de la Administración judicial electrónica la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso la auditoría del sistema de información y de su código fuente.

Los sistemas incluirán los indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica, cada uno en el ámbito de sus competencias.

Artículo 43. *Subsanación de actos procesales.*

1. El incumplimiento del deber de uso de las tecnologías, en los términos establecidos en esta Ley, por un profesional de la justicia en su primera comunicación con un órgano judicial podrá ser subsanado. A estos efectos, el órgano judicial concederá un plazo máximo de cinco días con apercibimiento de que todas sus actuaciones ante ese órgano, en ese o en cualquier otro proceso, así como ante cualquier otro órgano del mismo partido judicial, deberán realizarse empleando medios electrónicos y de conformidad con esta Ley.

2. Si la subsanación no se efectuase en el plazo señalado en el anterior apartado, no se admitirá la actuación que se tratara de realizar.

3. No será preciso practicar el requerimiento a que se refiere el apartado 1 del presente artículo cuando el profesional hubiera sido requerido en tal sentido por cualquier otro órgano judicial del mismo partido judicial, rechazándose de plano cualquier actuación que se tratara de efectuar por medios distintos a los previstos en la presente Ley.

TÍTULO V

Cooperación entre las Administraciones con competencias en materia de Administración de Justicia. El Esquema judicial de interoperabilidad y seguridad

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 44. *El Comité técnico estatal de la Administración judicial electrónica.*

1. El Comité técnico estatal de la Administración judicial electrónica estará integrado por una representación del Ministerio de Justicia y de cada una de las Comunidades Autónomas con competencias en la materia y por los representantes que al efecto podrán designar el Consejo General del Poder Judicial y la Fiscalía General del Estado.

Este Comité técnico estará copresidido por un representante del Consejo General del Poder Judicial y otro del Ministerio de Justicia.

2. Sin perjuicio de las competencias del Consejo General del Poder Judicial como garante de la compatibilidad de sistemas informáticos, este Comité tendrá las siguientes funciones:

a) Favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados por la Administración de Justicia.

b) Preparar planes y programas conjuntos de actuación para impulsar el desarrollo de la Administración judicial electrónica, respetando en todo caso las competencias autonómicas atinentes a los medios materiales de la Administración de Justicia.

c) Promover la cooperación de otras Administraciones públicas con la Administración de Justicia para suministrar a los órganos judiciales, a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, la información que precisen en el curso de un proceso judicial en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y en las leyes procesales.

d) Aquellas otras que legalmente se determinen.

Artículo 45. *Funcionamiento integrado y conjunto de todas las aplicaciones informáticas.*

El Comité técnico estatal de la Administración judicial electrónica fijará las bases para el desarrollo del Esquema judicial de interoperabilidad y seguridad de modo que permita, a través de las plataformas tecnológicas necesarias, la interoperabilidad total de todas las aplicaciones informáticas al servicio de la Administración de Justicia.

CAPÍTULO II

Esquema judicial de interoperabilidad y seguridad

Sección 1.ª Interoperabilidad judicial

Artículo 46. *Interoperabilidad de los sistemas de información.*

1. La Administración de Justicia utilizará las tecnologías de la información aplicando medidas informáticas, tecnológicas, organizativas y de seguridad que aseguren un adecuado nivel de interoperabilidad técnica, semántico-jurídica y organizativa entre todos los sistemas y aplicaciones que prestan servicios a la Administración de Justicia.

2. En el desarrollo de la actividad de la oficina judicial será obligatorio el uso de los servicios y consultas ofrecidos a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, salvo que existan razones técnicas que impidan su utilización.

Los programas y aplicaciones informáticos que se utilicen en la Administración de Justicia deberán ser previamente aprobados por el Consejo General del Poder Judicial, a los efectos de asegurar su compatibilidad con las funciones que le encomienda el artículo 230.5 de la Ley Orgánica del Poder Judicial.

Artículo 47. *Esquema judicial de interoperabilidad y seguridad.*

1. El Esquema judicial de interoperabilidad y seguridad será aplicado en la Administración de Justicia para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

2. El Esquema judicial de interoperabilidad y seguridad comprenderá:

a) El conjunto de criterios y recomendaciones en materia de seguridad, conservación, normalización y volcado de datos de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las distintas instituciones y Administraciones competentes para la toma de decisiones tecnológicas que aseguren la interoperabilidad.

b) La política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley y el establecimiento de los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3. En su elaboración se tendrá en cuenta lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones competentes en materia de justicia y los servicios electrónicos e infraestructuras ya existentes. A estos efectos utilizarán preferentemente estándares abiertos, así como, en su caso y de forma complementaria, considerarán el uso de estándares que sean de uso generalizado por los ciudadanos.

Artículo 48. *La interoperabilidad y la seguridad como cualidades integrales.*

1. Tanto la interoperabilidad como la seguridad se tendrán presentes de forma integral desde la concepción de los servicios, sistemas y aplicaciones a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

2. En el caso de la seguridad judicial, se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, atendiendo en todo caso a la especial sensibilidad de la información contenida en los procedimientos judiciales electrónicos.

Artículo 49. *Normas de conformidad.*

1. La interoperabilidad y la seguridad de las sedes y registros judiciales electrónicos, así como las del acceso electrónico de los ciudadanos a los servicios judiciales, se regirán por lo establecido en la presente Ley.
2. La conformidad con el Esquema judicial de interoperabilidad y seguridad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.
3. El Comité técnico estatal de Administración judicial electrónica velará por el establecimiento de los mecanismos de control para asegurar, de forma efectiva, el cumplimiento del Esquema judicial de interoperabilidad y seguridad.
4. En las sedes judiciales electrónicas correspondientes se publicarán las declaraciones de conformidad, compatibilidad y otros posibles distintivos de interoperabilidad obtenidos respecto al cumplimiento del Esquema judicial de interoperabilidad y seguridad.

Artículo 50. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Artículo 51. *Desarrollo del marco normativo técnico.*

Para el mejor cumplimiento de lo establecido en relación con el Esquema judicial de interoperabilidad y seguridad, el Comité técnico estatal de la Administración judicial electrónica, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones. El Consejo General del Poder Judicial aprobará las guías cuando afecten a la compatibilidad de los sistemas informáticos en los términos previstos en el artículo 230.5 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Artículo 52. *Actualización permanente.*

1. El Esquema judicial de interoperabilidad y seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de administración electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Para ello, se desarrollarán las correspondientes guías y normas técnicas de aplicación.
2. Corresponde al Comité técnico estatal de la Administración judicial electrónica aprobar las bases para la actualización del Esquema judicial de interoperabilidad y seguridad.

Sección 2.ª Seguridad judicial electrónica

Artículo 53. *Elementos básicos de la seguridad judicial electrónica.*

1. En las decisiones en materia de seguridad judicial electrónica deberán tenerse en cuenta los siguientes elementos:

a) La seguridad integral, desde el punto de vista de un proceso integral constituido por los elementos organizativos, normativos, humanos y técnicos relacionados con el sistema.
b) La gestión de riesgos, como proceso de garantía de la seguridad de la información.
c) La prevención, detección, reacción, corrección y recuperación como procesos soporte a la seguridad de la información.
d) Los niveles de seguridad, entendidos como capas de seguridad que permitan una gestión de incidentes más adecuada.

e) La reevaluación periódica de las medidas de seguridad existentes para adecuar su eficacia a la constante evolución de riesgos, tecnología y sistemas de protección.

f) La función diferenciada dentro de la organización, estableciendo una estructura organizativa donde se identifiquen las figuras de responsable de la información, responsable de seguridad y responsable del servicio prestado.

2. Son dimensiones de la seguridad judicial electrónica:

a) Autenticidad.
b) Confidencialidad.
c) Integridad.
d) Disponibilidad.
e) Trazabilidad.
f) Conservación.

Artículo 54. *Requisitos mínimos de seguridad.*

El Esquema judicial de interoperabilidad y seguridad fijará los requisitos mínimos que todas las instituciones judiciales han de garantizar en relación a los sistemas de información de los que son responsables. Estos requisitos se desarrollarán mediante una guía técnica.

CAPÍTULO III

Reutilización de aplicaciones y transferencia de tecnologías. Directorio general de información tecnológica judicial

Artículo 55. *Reutilización de sistemas, infraestructuras y aplicaciones de propiedad de las Administraciones de Justicia.*

1. Las Administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, podrán ponerlas a disposición de cualquier institución judicial o cualquier Administración pública sin contraprestación y sin necesidad de convenio.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración de Justicia. Se publicarán, en tal caso, como licencia pública de la Unión Europea, sin perjuicio de otras licencias que aseguren que los programas, datos o información que se comparten:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios, siempre que la obra derivada mantenga estas mismas cuatro garantías.

3. En el desarrollo de las soluciones para la Administración de Justicia se fomentará la reutilización de los sistemas, servicios, infraestructuras y aplicaciones existentes, siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

Artículo 56. *Transferencia de tecnología entre Administraciones. Directorio General de información tecnológica judicial.*

1. El Ministerio de Justicia mantendrá un directorio general de aplicaciones judiciales para su reutilización e impulsará el mantenimiento del mismo, en colaboración con el resto de Administraciones competentes en materia de justicia. Se promoverá el desarrollo de guías técnicas, formatos y estándares comunes de especial interés para el desarrollo de la Administración judicial electrónica en el marco institucional de cooperación en materia de administración electrónica.

2. Las Administraciones mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el desarrollo

de la administración electrónica y de conformidad con lo que al respecto se establezca en el marco institucional de cooperación en materia de administración electrónica.

3. Las instituciones judiciales deberán tener en cuenta las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados.

Disposición adicional primera. *Creación del Comité técnico estatal de la Administración judicial electrónica.*

La estructura, composición y funciones del Comité técnico estatal de la Administración judicial electrónica serán establecidas reglamentariamente por el Gobierno, mediante Real Decreto, previo informe del Consejo General del Poder Judicial, de la Fiscalía General del Estado, de la Agencia Española de Protección de Datos y de las Comunidades Autónomas con competencias en la materia.

Disposición adicional segunda. *Adaptación a los sistemas de administración electrónica.*

Para garantizar la efectividad del derecho a la tutela judicial reconocida en el artículo 24 de la Constitución, en el plazo de cinco años desde la entrada en vigor de esta Ley las Administraciones con competencia en materia de Administración de Justicia dotarán a las oficinas judiciales y fiscalías de sistemas de gestión procesal que permitan la tramitación electrónica de los procedimientos.

Disposición adicional tercera. *Interoperabilidad entre las aplicaciones de la Administración de Justicia.*

En el plazo de cuatro años desde la entrada en vigor de la presente Ley, las Administraciones con competencia en materia de Administración de Justicia garantizarán la interoperabilidad entre los sistemas al servicio de la Administración de Justicia, de acuerdo a las especificaciones establecidas por el Comité técnico estatal de Administración judicial electrónica en el marco institucional de cooperación en materia de administración electrónica.

Disposición adicional cuarta. *Accesibilidad a los servicios electrónicos.*

Las Administraciones con competencias en materia de justicia garantizarán que todos los ciudadanos, con especial atención a las personas mayores o con algún tipo de discapacidad, que se relacionan con la Administración de Justicia puedan acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos. Las características de los medios que permitan la universalización del acceso a los servicios electrónicos serán desarrolladas reglamentariamente por el Gobierno, mediante Real Decreto, previo informe de las Comunidades Autónomas con competencias en la materia.

Disposición adicional quinta. *Dotación de medios e instrumentos electrónicos y sistemas de información.*

Las Administraciones competentes en materia de Justicia dotarán a todos los órganos, oficinas judiciales y fiscalías de los medios e instrumentos electrónicos y de los sistemas de información necesarios y suficientes para poder desarrollar su función eficientemente. Estos sistemas serán plenamente accesibles y operativos sin necesidad de que los usuarios se encuentren físicamente en las sedes de sus respectivos órganos, oficinas o fiscalías, con respeto a las políticas internas que garanticen el derecho a la desconexión digital recogido en el artículo 14.j.bis y en el artículo 88 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre. Asimismo, formarán a los integrantes de los mismos en el uso y utilización de dichos medios e instrumentos.

Disposición adicional sexta. *Representantes procesales del Estado y demás entes públicos.*

1. A los efectos señalados en el artículo 24, y, en general, de aplicación de esta Ley a la actuación procesal de los abogados del Estado, representantes procesales del Estado y demás entes públicos a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, se suscribirá un protocolo de actuación.

2. Las Administraciones competentes en materia de justicia dotarán a los órganos y oficinas de los representantes del Estado y demás entes públicos a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, de los medios e instrumentos electrónicos necesarios y suficientes para poder desarrollar su función eficientemente. Asimismo, formarán a los integrantes de los mismos en el uso y utilización de dichos medios e instrumentos.

Disposición adicional séptima. *Legislación aplicable.*

La presente Ley tiene carácter transversal para todos los órdenes jurisdiccionales y complementará la legislación vigente en lo concerniente al uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Disposición adicional octava. *Legislación aplicable en materia de interoperabilidad.*

En lo no previsto en esta Ley, los criterios de interoperabilidad para las relaciones entre la Administración de Justicia y las Administraciones públicas, así como las entidades sujetas a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, se regirán conforme a lo contemplado en esta última.

Disposición adicional novena. *Aplicación de la Ley al Ministerio Fiscal.*

Las referencias contenidas en el texto y articulado de la presente Ley a las oficinas judiciales, actividad judicial, juzgados y tribunales, sede judicial electrónica, órganos judiciales, expediente judicial electrónico, documento judicial electrónico, registro judicial electrónico y procedimiento judicial, serán de aplicación equivalente y se entenderán referidas igualmente a las oficinas fiscales, actividad fiscal, fiscalías, sedes fiscales electrónicas, expedientes fiscales electrónicos, registros fiscales electrónicos y procedimientos de cualquier tipo que se realicen y tramiten por el Ministerio Fiscal.

Disposición adicional décima. *Aplicación de la Ley en el ámbito de la jurisdicción militar.*

Las disposiciones contenidas en la presente Ley serán de aplicación en el ámbito de la jurisdicción militar, sin perjuicio de las especialidades propias de sus normas reguladoras.

Disposición adicional undécima. *Declaración de requerimientos tecnológicos de las reformas en las leyes procesales.*

Todo proyecto de ley que disponga o incluya reformas en las leyes procesales podrá ir acompañado de una declaración de requerimientos tecnológicos para su correcta implantación y aplicación.

Disposición adicional duodécima. *Relaciones de colaboración con los Colegios de Procuradores.*

Sin perjuicio de lo establecido en esta Ley y en especial de lo dispuesto en el Capítulo III de su Título IV, las relaciones de colaboración con los Colegios de Procuradores en el desempeño de las funciones que se les encomiendan para la organización de los servicios de notificaciones y traslados de copias previas para con estos profesionales de acuerdo con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en la Ley de Enjuiciamiento Civil, podrán ser objeto del correspondiente y oportuno desarrollo en un convenio que se suscribirá con el Consejo General de Colegios de Procuradores de España, que recoja los presupuestos básicos de la presente Ley para la utilización de las tecnologías de la información en sus relaciones con la Administración de Justicia.

Disposición adicional decimotercera. *Publicaciones en el Tablón Edictal Judicial Único.*

Las publicaciones que, en cumplimiento de lo previsto en las leyes procesales, deban hacerse en el Tablón Edictal Judicial Único serán gratuitas en todo caso, sin que proceda contraprestación económica por parte de quienes la hayan solicitado.

Igualmente serán gratuitas las consultas en el tablón, así como las suscripciones que los ciudadanos puedan realizar en su sistema de alertas.

Disposición transitoria primera. *Coexistencia de procedimientos.*

1. Durante el tiempo en que coexistan procedimientos tramitados en soporte papel con procedimientos tramitados exclusivamente en formato electrónico, los servicios electrónicos de información del estado de la tramitación a que se refiere la presente Ley incluirán, respecto a los primeros, al menos la fase en la que se encuentra el procedimiento y el órgano o unidad responsable de su tramitación.

2. Los registros electrónicos existentes a la entrada en vigor de la presente Ley serán considerados registros judiciales electrónicos, regulándose por lo dispuesto en los artículos 30, 31 y 32 de esta Ley.

Disposición transitoria segunda. *Expediente electrónico con valor de copia simple.*

Si el estado de la técnica no hiciera posible remitir el expediente administrativo electrónico con los requisitos establecidos en su normativa específica, de conformidad con lo señalado en el apartado 4 del artículo 37 de esta Ley, dicho expediente tendrá el valor de copia simple. Será admisible la remisión del expediente en formato papel si las condiciones técnicas no permitiesen su remisión telemática.

Disposición transitoria tercera. *Tablón Edictal Judicial Único.*

La publicación de los edictos mediante el Tablón Edictal Judicial Único resultará de aplicación a partir del 1 de junio de 2021 tanto a los procedimientos que se inicien con posterioridad, como a los ya iniciados.

Disposición final primera. *Título competencial.*

La presente Ley se dicta al amparo de lo dispuesto en el artículo 149.1.5.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de Administración de Justicia.

Disposición final segunda. *Desarrollo normativo.*

Corresponde al Gobierno y a las Comunidades Autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y aplicación de la presente Ley.

Disposición final tercera. *Regulación del uso de los sistemas de videoconferencia en la Administración de Justicia.*

El Gobierno presentará un proyecto de ley que regule de manera integral el uso de los sistemas de videoconferencia en la Administración de Justicia.

Disposición final cuarta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Definiciones

A efectos de la presente Ley, se entiende por:

– Actividad de servicio: Cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración.

– Actuación judicial automatizada: Actuación judicial producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

– Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de la informática.

– Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

– Autenticación: Acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos y de la integridad y autoría de estos últimos.

– Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Canales: Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc.).

– Certificado electrónico: Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

– Certificado electrónico reconocido: Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que preste.

– Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Disponibilidad: Propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

– Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

– Espacios comunes o ventanillas únicas: Modos o canales (oficinas integradas, atención telefónica, páginas en Internet y otros) a los que los ciudadanos pueden dirigirse para acceder a las informaciones, trámites y servicios públicos determinados por acuerdo entre varias Administraciones.

– Estándar abierto: Aquel que reúna las siguientes condiciones:

Sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

– Firma electrónica: Según el apartado 1 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

– Firma electrónica avanzada: Según el apartado 2 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

– Firma electrónica reconocida: Según el apartado 3 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

– Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

– Infraestructuras y servicios comunes: Instrumentos operativos que facilitan el desarrollo y despliegue de nuevos servicios, así como la interoperabilidad de los existentes, creando escenarios de relación multilateral y que satisfacen las necesidades comunes en los distintos ámbitos administrativos; son ejemplos la Red de comunicaciones de las Administraciones públicas españolas, la Red transeuropea sTESTA y la plataforma de verificación de certificados electrónicos.

– Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

– Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

– Interoperabilidad semántico-jurídica: Es aquella dimensión de la interoperabilidad relativa a que la información, en el ámbito o de carácter judicial, intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

– Interoperabilidad técnica: Aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

– Licencia pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las veintitrés lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

– Medidas de seguridad: Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción o de recuperación.

– Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

– Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

– Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

– Prestador de actividad de servicio: Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

– Punto de acceso electrónico: Conjunto de páginas web agrupadas en un dominio de Internet cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios dirigidos a resolver necesidades específicas de un grupo de personas o el acceso a la información y servicios de una institución pública.

– Requisitos mínimos de seguridad: Exigencias necesarias para asegurar la información y los servicios.

– Sistema de firma electrónica: Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

– Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

– Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

– Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

– Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

§ 23

Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia

Ministerio de Justicia
«BOE» núm. 33, de 7 de febrero de 2009
Última modificación: 30 de diciembre de 2015
Referencia: BOE-A-2009-2073

Por Real Decreto de 2 de octubre de 1878 se dispuso ya el establecimiento en el Ministerio de Gracia y Justicia de un Registro Central de Procesados y otro de Penados, consecuencia de la necesidad de satisfacer un fin jurídico elemental: hacer posible la demostración de la reincidencia para la aplicación más justificada de los correspondientes preceptos del Código Penal, así como para poder establecer las medidas cautelares necesarias que aseguraran la presencia del inculpado en el juicio.

La promulgación de leyes generales de tanta trascendencia pública y privada como son la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, constituyen elementos determinantes en su evolución. Por otro lado, los acuerdos o convenios suscritos con Estados en ámbitos de cooperación bilateral o multilateral y las normas comunitarias obligan al Registro a una continua evaluación de sus procedimientos, innovándolos cuando sea necesario, pero con respeto a los principios a que responde su creación.

Con posterioridad, y en virtud de los Reales Decretos 231/2002, de 1 de marzo, 232/2002, de 1 de marzo y 355/2004, de 5 de marzo, entraron en funcionamiento los Registros Centrales de Rebeldes Civiles, de Sentencias de Responsabilidad Penal de los Menores y para la Protección de las Victimas de Violencia Doméstica.

El Plan de Transparencia Judicial, aprobado por Acuerdo del Consejo de Ministros de 25 de octubre de 2005, establece dentro de sus objetivos la mejora del sistema de Registros Judiciales, que constituye un referente ineludible para el ejercicio eficaz de las funciones que, en materia penal, y en el caso del Registro Central de Rebeldes Civiles, en materia civil, las leyes atribuyen a la Administración de Justicia.

La consecución de este objetivo pasa por proporcionar a los jueces, fiscales, secretarios judiciales y policía judicial nuevas herramientas de trabajo que faciliten el manejo de la información y permita que determinados usuarios -previamente definidos, en función del tipo de información que van a manejar- tengan un conocimiento completo de la información que precisan para el ejercicio de las funciones que tienen encomendadas y para la correcta toma de decisiones.

Ahora, como novedad más destacada, mediante este real decreto, se lleva a cabo la creación y puesta en funcionamiento del Registro de Medidas Cautelares, Requisitorias y

Sentencias no Firmes, previsto en la disposición adicional segunda de la Ley de Enjuiciamiento Criminal, que, en el orden jurisdiccional penal, constituirá un instrumento de gran utilidad que permitirá al órgano judicial disponer de otros elementos de juicio, además de los ya existentes, a fin de ponderar sus resoluciones en las distintas fases del proceso penal. Igualmente es importante ofrecer información sobre la existencia de órdenes en vigor de busca y captura o de detención y puesta a disposición, que permiten al Juez valorar la existencia de riesgo de fuga, en la resolución en la que decida sobre la prisión o libertad provisional del imputado, tal como se establece en el artículo 503.1.3º a), párrafo 3.º de la Ley de Enjuiciamiento Criminal de 14 de septiembre de 1882.

La peligrosidad del sujeto es un dato fundamental a la hora de individualizar la pena en la sentencia, ya que el Juez debe tener en cuenta al imponer aquélla no sólo la gravedad del hecho, sino también las circunstancias personales del culpable, conforme a lo dispuesto en el artículo 66.1.6.º de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, y para la concesión del beneficio de suspensión de la condena no sólo es necesario que se cumplan los requisitos que se determinan en el artículo 81 del Código Penal, sino que es preciso que el Tribunal también tenga en cuenta la peligrosidad del sujeto, así como la existencia de otros procedimientos penales contra éste, de conformidad con el artículo 80.1 del mismo texto legal, para lo que puede ser un dato fundamental si se encuentra en prisión provisional o sufriendo otra medida cautelar en causa penal distinta. También para el instituto de la sustitución de las penas de prisión por las de localización permanente o de multa, es preciso tener en cuenta las circunstancias personales del reo, y su conducta, tal como prevé el artículo 88.1 del Código Penal, para cuya valoración es igualmente preciso conocer si se encuentra incurso en otras causas criminales por delito, y si en esas causas se han acordado medidas cautelares contra él.

Además, aunque este Registro no está concebido como registro específico de agresores sexuales, sin duda alguna su puesta en funcionamiento contribuirá a prevenir la especial reincidencia que se produce en estos tipos delictivos. Por otro lado, uno de los objetivos perseguidos es la protección específica de las víctimas de delitos contra la libertad e indemnidad sexual que sean menores de edad. Así, uno de los aspectos novedosos que reflejará la información contenida en el Registro será precisamente la condición de menor de edad de las víctimas de esta clase de delitos, proporcionando tanto a los Juzgados y Tribunales como a la Policía Judicial nuevos elementos de conocimiento que permitan una protección más eficaz de los menores.

Estas, y otras muchas razones, avalan la necesidad de organizar este nuevo Registro, no en forma aislada sino en un conjunto organizado que constituya un sistema de información integrado en el que los distintos usuarios puedan obtener, en función del acceso que les ha sido concedido, una información adecuada a sus necesidades, rápida y veraz.

Todo lo expuesto justifica la conveniencia de publicar una norma en la que, en un sistema único, se recojan y sistematicen todas las disposiciones, con frecuencia obsoletas, que regulan las competencias, organización y ámbito de actuación de diferentes Registros. La finalidad pretendida es que desde un único punto los Juzgados y Tribunales gestionen, tanto la incorporación de datos a los distintos Registros como las consultas que realicen. En un periodo razonable, se logrará que la información acceda a los Registros mediante el volcado de datos desde el sistema de gestión procesal, de ese modo el tiempo invertido en la gestión ordinaria de los expedientes servirá para la inscripción en el Registro. Al mismo tiempo, se establece para todos los Registros que la trasmisión y el acceso a la información contenida en los mismos se realice a través de procedimientos telemáticos.

En definitiva, este Sistema de registros administrativos de apoyo a la Administración de Justicia, tiene como objeto principal servir de apoyo a la actividad de los órganos judiciales e impulsar su modernización. Al mismo tiempo, se persigue contribuir a la conexión del Sistema de registros con los Registros de otros países de la Unión Europea conforme a lo previsto en la Decisión 2005/876/JAI del Consejo, de 21 de noviembre de 2005 y la propuesta de Decisión Marco del Consejo relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros.

El real decreto dedica el capítulo I a establecer una serie de disposiciones generales sobre el objeto y naturaleza del Sistema de registros, destacando su carácter no público y su

dependencia del Ministerio de Justicia. El artículo tercero se refiere a la inscripción de la información procedente de órganos judiciales extranjeros y el artículo cuarto a la organización del Sistema integrado.

El capítulo II establece quienes pueden acceder a los diferentes niveles de información en función del perfil adjudicado.

El capítulo III detalla la información que debe contenerse en cada uno de los Registros y los plazos para el envío de la misma. Como novedad destacada, se ha optado por incluir los autos de rebeldía dentro de la información que debe inscribirse en el Registro de Medidas Cautelares, Requisitorias y Sentencias No Firmes al entender que la declaración de rebeldía puede adoptarse en distintas fases del procedimiento.

Las medidas de seguridad del Sistema y de los datos contenidos en el mismo, de conformidad con lo previsto en la legislación sobre protección de datos, son objeto de regulación en el capítulo IV.

El capítulo V se ocupa de la emisión del certificado de las inscripciones contenidas en el Sistema de registros administrativos de apoyo a la Administración de Justicia. Se regula su emisión a instancia del titular, extremando las cautelas con el fin de evitar que los datos registrales sean obtenidos por persona diferente del afectado. Se establece el procedimiento de la certificación de datos penales obtenidos directamente por los órganos judiciales, respecto a las causas que se tramiten en los juzgados; eliminando trámites burocráticos sin ninguna merma de la seguridad jurídica y regulando el marco de colaboración entre administraciones públicas, en línea con lo que se establece en la Ley 30/1992 de 26 de noviembre.

El capítulo VI desarrolla cuestiones relativas a la cancelación de inscripciones. De este modo, se ha podido regular de forma unitaria algunos aspectos importantes del sistema registral, con las particularidades propias de cada tipo de asiento y respetando, por lo que a los antecedentes penales se refiere, la regulación contenida en el artículo 136 del Código Penal. Concluye el real decreto con una referencia a la elaboración de la información estadística que de los datos contenidos en el sistema de Registros puede derivarse, información de calidad y de enorme significado que debe configurarse como un importante aspecto del Plan de Transparencia Judicial.

El presente real decreto ha sido informado por el Consejo General del Poder Judicial, la Fiscalía General del Estado, la Agencia Española de Protección de Datos, y el Consejo del Secretariado.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 6 de febrero de 2009,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto crear el sistema de registros administrativos de apoyo a la Administración de Justicia, y regular su organización y funcionamiento.

2. Dicho Sistema de registros estará integrado por el Registro Central de Penados, el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes, el Registro Central de Rebeldes Civiles, el Registro de Sentencias de Responsabilidad Penal de los Menores y el Registro Central de Delincuentes Sexuales.

Artículo 2. *Naturaleza del sistema de registros de apoyo a la Administración de Justicia.*

1. El sistema de registros constituye un sistema de información de carácter no público cuyo objetivo fundamental es servir de apoyo a la actividad de los órganos judiciales y del Ministerio Fiscal, de las Fuerzas y Cuerpos de Seguridad del Estado y Cuerpos de Policía de

las comunidades autónomas con competencias plenas en materia de seguridad pública, y de otros órganos administrativos, en el ámbito de las competencias delimitadas en el presente real decreto.

2. Su ámbito de actividad se extiende a todo el territorio nacional, sin perjuicio de lo dispuesto por los tratados internacionales suscritos en esta materia por España.

3. Este sistema, integrado por las bases de datos de los Registros que a continuación se relacionan, tiene por objeto, en cada caso:

a) Registro Central de Penados: la inscripción de las resoluciones firmes por la comisión de un delito o falta que impongan penas o medidas de seguridad, dictadas por los Juzgados o Tribunales del orden jurisdiccional penal.

b) Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes: La inscripción de penas y medidas de seguridad impuestas en sentencia no firme por delito o falta y medidas cautelares acordadas que no sean objeto de inscripción en el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, autos de declaración de rebeldía y requisitorias adoptadas en el curso de un procedimiento penal por los Juzgados o Tribunales del orden jurisdiccional penal, anotándose la fecha de notificación cuando la misma se produzca.

c) Registro Central para la Protección de las Víctimas de Violencia Doméstica: la inscripción de penas y medidas de seguridad impuestas en sentencia por delito o falta, medidas cautelares y órdenes de protección acordadas en procedimientos penales en tramitación, contra alguna de las personas a las que se refiere el artículo 173.2 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Asimismo, la inscripción de los quebrantamientos de cualquier pena, medida u orden de protección acordada en dichos procedimientos penales.

d) Registro Central de Rebeldes Civiles: la inscripción de demandados en cualquier procedimiento civil cuyo domicilio se desconozca y siempre que no hayan tenido resultado positivo las averiguaciones de domicilio a que se refiere el artículo 156 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

e) Registro Central de Sentencias de Responsabilidad Penal de los Menores: la inscripción de sentencias condenatorias firmes dictadas por los Juzgados y Tribunales en aplicación de la Ley Orgánica 5/2000, de 12 de enero, reguladora de la Responsabilidad Penal de los Menores.

f) Registro Central de Delincuentes Sexuales: la inscripción de la información relativa a quienes hayan sido condenados por sentencia judicial firme por los delitos contra la libertad e indemnidad sexuales, así como por trata de seres humanos con fines de explotación sexual, incluyendo la pornografía, de conformidad con la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.

4. Dependiendo del Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes y del Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, existirá un Fondo Documental de Requisitorias cuya creación y régimen jurídico queda establecido en la disposición adicional cuarta.

Artículo 3. *Información procedente de órganos jurisdiccionales extranjeros.*

Además de las sentencias y autos a que se refiere el apartado 3.a) del artículo anterior, se inscribirán en el Registro Central de Penados las siguientes sentencias firmes dictadas por los órganos jurisdiccionales extranjeros:

a) Las dictadas por los Juzgados y Tribunales de cualquier Estado extranjero, cuando así se determine por los tratados internacionales sobre esta materia suscritos por España.

b) Las dictadas por Juzgados y Tribunales europeos, de acuerdo con lo previsto en los tratados internacionales de asistencia judicial en materia penal suscritos por España y las disposiciones dictadas por la Unión Europea.

c) Las dictadas por Juzgados y Tribunales extranjeros cuando la ejecución de las mismas se realice en España. La inscripción se practicará a instancia del órgano judicial español que conozca de la ejecución.

Artículo 4. *Organización.*

1. La gestión de las bases de datos que integran el Sistema de registros administrativos de apoyo a la Administración de Justicia corresponde al Ministerio de Justicia, a través de la Secretaría de Estado de Justicia.

2. En cada Registro existirá un encargado, que será responsable de su organización y gestión, adoptará las medidas necesarias para asegurar su correcto funcionamiento, velará por la veracidad, confidencialidad e integridad de las inscripciones e impulsará el cumplimiento de lo previsto en materia de cancelaciones de las mismas.

CAPÍTULO II

Acceso a la información

Artículo 5. *Acceso general a la información contenida en el Sistema de Registros.*

1. El Ministerio de Justicia autorizará, estableciendo las medidas de seguridad oportunas, el acceso directo a la información contenida en los Registros Centrales integrados en el Sistema, a:

a) Los órganos judiciales, a través del personal de cada oficina judicial autorizado por el Secretario Judicial, a los efectos de su utilización en los procedimientos y actuaciones de los que están conociendo en el ámbito de sus respectivas competencias, conforme a las disposiciones legales vigentes.

b) El Ministerio Fiscal, a través del personal de cada Fiscalía autorizado por el Fiscal Jefe, cuando ello resulte necesario para el cumplimiento de las funciones atribuidas al mismo por la Ley de Enjuiciamiento Criminal aprobada por real decreto de 14 de septiembre de 1882, la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad Penal de los menores y la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal.

2. En cualquier caso, los interesados, acreditando su identidad, tendrán derecho a solicitar el acceso, mediante exhibición, únicamente a los datos relativos a su persona contenidos en cualquiera de los Registros a los que se refiere este real decreto.

Articulo 6. *Acceso a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes.*

1. Además de los indicados en el artículo anterior, el Ministerio de Justicia autorizará, estableciendo las medidas de seguridad oportunas, el acceso directo a la información contenida en el Registro Central de Penados y en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes, siempre que en uno y otro caso se refiera a inscripciones no canceladas, a:

a) La policía judicial, a través de los funcionarios autorizados que desempeñen estas funciones, en tanto sea necesario para el ejercicio de las competencias previstas en el artículo 549.1 de la Ley Orgánica del Poder Judicial.

b) Las unidades de Intervención de Armas y Explosivos de la Guardia Civil responsables de la concesión de los permisos de armas, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

c) Las unidades del Cuerpo Nacional de Policía responsables de la expedición del pasaporte, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

d) Las unidades del Cuerpo Nacional de Policía responsables del control de entrada y salida del territorio nacional, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

2. El encargado del Registro Central de Penados y el del Registro deMedidas Cautelares, Requisitorias y Sentencias no firmes comunicará al menos semanalmente a la Dirección General de Tráfico del Ministerio del Interior los datos relativos a penas, medidas de seguridad y medidas cautelares en las que se haya dispuesto la privación del derecho a

conducir vehículos a motor y ciclomotores o cualquier pena o medida relacionada con la seguridad vial, de acuerdo con lo previsto en los artículos 529 bis, 765.4 y 794.2 y concordantes de la ley de Enjuiciamiento Criminal.

Articulo 7. *Acceso a la información contenida en el Registro Central de Protección a las Victimas de Violencia Doméstica.*

1. Además de los indicados en el artículo 5, el Ministerio de Justicia autorizará, estableciendo las medidas de seguridad oportunas, el acceso directo a la información contenida en el Registro Central de Protección a las Víctimas de Violencia Doméstica, a:

a) La policía judicial, a través de los funcionarios autorizados que desempeñen estas funciones, en tanto sea necesario para el ejercicio de las competencias previstas en el artículo 549.1 de la Ley Orgánica del Poder Judicial.

b) Las unidades de Intervención de Armas y Explosivos de la Guardia Civil responsables de la concesión de los permisos de armas, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

c) Las unidades del Cuerpo Nacional de Policía responsables de la expedición del pasaporte, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

d) Las unidades del Cuerpo Nacional de Policía responsables del control de entrada y salida del territorio nacional, a través de los funcionarios autorizados en relación con los fines que tienen encomendados.

e) Las unidades de policía especialmente encargadas del control y seguimiento de la violencia doméstica, exclusivamente en el ámbito de sus competencias de protección de víctimas de violencia doméstica o de género, a través de los funcionarios autorizados.

f) Las comunidades autónomas, exclusivamente en el ámbito de sus competencias de protección de las víctimas de violencia doméstica o de género, a través del responsable del punto de coordinación o, en su caso, a través de las personas designadas por dicho responsable. Este acceso directo se entenderá sin perjuicio de las comunicaciones previstas por la disposición adicional primera de este real decreto.

g) Las delegaciones y subdelegaciones del Gobierno, exclusivamente en el ámbito de sus competencias de protección de víctimas de violencia doméstica o de género. En el caso de las delegaciones del Gobierno, a través del responsable de la unidad de coordinación contra la violencia sobre la mujer o las personas que éste designe; en el caso de las subdelegaciones del Gobierno, a través del responsable de la unidad contra la violencia sobre la mujer o las personas que éste designe.

h) La Administración Penitenciaria, exclusivamente en el ámbito de sus competencias de protección de las víctimas de la violencia doméstica o de género, a través de los funcionarios autorizados.

2. El encargado del Registro Central de Protección de Víctimas de Violencia Doméstica comunicará al menos semanalmente al Instituto Nacional de la Seguridad Social, al Instituto Social de la Marina y a la Dirección General de Costes de Personal y Pensiones Públicas del Ministerio de Economía y Hacienda la información relativa a los procedimientos terminados por sentencia firme condenatoria que se inscriban en dicho Registro por la comisión de un delito doloso de homicidio en cualquiera de sus formas o de lesiones cuando la ofendida por el delito fuera cónyuge o ex cónyuge del condenado o estuviera o hubiera estado ligada a él por una análoga relación de afectividad a efectos de dar cumplimiento a lo previsto en la disposición adicional primera de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Genero.

3. El encargado del Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género comunicará al menos semanalmente a la Dirección General de Tráfico del Ministerio del Interior los datos relativos a penas, medidas de seguridad y medidas cautelares en las que se haya dispuesto la privación del derecho a conducir vehículos a motor y ciclomotores o cualquier pena o medida relacionada con la seguridad vial, de acuerdo con lo previsto en los artículos 529 bis, 765.4 y 794.2 y concordantes de la Ley de Enjuiciamiento Criminal.

CAPÍTULO III

Información contenida en el sistema

Artículo 8. *Información de carácter general contenida en los Registros integrados en el Sistema.*

La información contenida en los Registros Centrales integrados en el Sistema deberá comprender, con carácter general, los siguientes datos:

a) Datos identificativos.

Nombre y apellidos del condenado, rebelde, sometido a medidas de seguridad o medida cautelar, alias en su caso, sexo, fecha de nacimiento, nombre de los padres, localidad, provincia, país de nacimiento, domicilio conocido, nacionalidad y documento nacional de identidad o NIE, pasaporte o tarjeta de identidad en el caso de los extranjeros, número ordinal informático policial y número de atestado.

En relación con las personas jurídicas se hará constar la razón o denominación social, nacionalidad, domicilio social y domicilio fiscal, actividad principal, tipo de sociedad, número o código de identificación fiscal y datos registrales.

En el supuesto de entes sin personalidad jurídica se hará constar denominación, número o código de identificación fiscal o cualquier otro dato que sirva para su identificación.

Cuando en una misma causa resulten condenadas personas físicas y personas jurídicas o entes sin personalidad se hará contar esta circunstancia en el Sistema de registros de apoyo a la Administración de Justicia.

b) Órgano judicial que acuerda la resolución, fecha de la misma, clase y número de procedimiento, y número de identificación general.

c) Los datos personales identificativos de la víctima, domicilio o domicilios conocidos de la víctima, y relación de parentesco entre la víctima y el condenado o denunciado siempre que sea necesario y, en todo caso, en los procedimientos de violencia doméstica o de género.

d) La condición de menor de edad de la víctima cuando se trate de delitos contra la libertad e indemnidad sexuales.

Artículo 9. *Información contenida en la inscripción de sentencias firmes.*

Cuando se trate de sentencias firmes que impongan penas o medidas de seguridad a personas físicas mayores de edad, penas a personas jurídicas o consecuencias accesorias a entes sin personalidad se inscribirán, además, los siguientes datos:

a) Fecha de la sentencia que imponga la pena o medida de seguridad.

b) Fecha de firmeza de la sentencia y fecha de efectos del requerimiento del cumplimiento.

c) Órgano judicial sentenciador.

d) Condición de reincidente y/o reo habitual del condenado en su caso.

e) Órgano judicial de ejecución de la sentencia, en su caso.

f) Número y año de la ejecutoria.

g) Delito o delitos y precepto penal aplicado.

h) Pena o penas principales y accesorias, medida de seguridad y su duración y cuantía de la multa con referencia a su duración y cuota diaria o multa proporcional.

i) Fecha de comisión del delito.

j) Participación como autor o cómplice y grado de ejecución.

k) Sustitución de las penas o medidas de seguridad, en su caso.

l) Suspensión de la ejecución de las penas o medidas de seguridad, en su caso, fecha de notificación, así como plazo por el que se concede la suspensión.

m) Prórroga del auto de suspensión de las penas.

n) Fecha de la revocación del auto de suspensión de las penas o medidas de seguridad.

ñ) Fecha de la remisión definitiva de la pena, cumplimiento efectivo de la misma o prescripción.

o) Fecha del cese de la medida de seguridad.

p) Expulsión y fecha de la misma, cuando se acuerde como sustitución de la pena o medida de seguridad.

q) Cumplimiento.

r) Acumulación de penas.

s) Responsabilidad civil derivada de la infracción penal.

t) Resoluciones judiciales que se pronuncien sobre el traslado de la pena de acuerdo con el artículo 130.2 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Artículo 10. *Información contenida en la inscripción de medidas cautelares, requisitorias, autos de rebeldía o sentencias no firmes.*

Cuando se trate de medidas cautelares, requisitorias, autos de rebeldía o Sentencias No Firmes impuestas a personas físicas mayores de edad y, en su caso, a personas jurídicas y entes sin personalidad se inscribirán, además, los siguientes datos:

a) Medidas cautelares, personales o reales y órdenes de protección en los procedimientos de violencia doméstica o de género, indicando fecha de adopción, de notificación al sometido a la medida u orden de protección y de cancelación y, en su caso tipo, contenido, ámbito y duración, así como sus modificaciones o sustituciones, y delito o falta objeto del procedimiento. En relación con las órdenes de protección se indicará la situación y origen de la solicitud.

b) Sentencias No Firmes indicando órgano enjuiciador, procedimiento, fecha de la misma y, en su caso, delitos o faltas declaradas, penas o medidas de seguridad impuestas, su duración o cuantía.

c) Órdenes de busca, indicando el órgano judicial que la acuerda, fecha de la misma, tipo de procedimiento, delito objeto del procedimiento, pena y duración de la misma.

d) Órdenes europeas de detención y entrega emitidas por las autoridades judiciales españolas.

e) Auto de rebeldía indicando fecha del auto y de su anulación.

Artículo 11. *Información contenida en las inscripciones en el Registro Central de Sentencias Firmes de Menores.*

Cuando se trate de inscripciones en el Registro Central de Sentencias Firmes de Menores, se inscribirán, además, los siguientes datos:

a) Fecha en que adquiere firmeza la sentencia, así como la suspensión, reducción o sustitución de la medida que acuerde el Juez mediante auto motivado, cuando éste sea firme, y demás datos de la ejecutoria.

b) Las medidas impuestas al menor, su duración y, en su caso, el lugar de cumplimiento.

c) La fecha de prescripción, de cumplimiento o finalización por cualquier causa de la medida o medidas impuestas.

Artículo 12. *Información contenida en las inscripciones en el Registro Central de Rebeldes Civiles.*

Cuando se trate de inscripciones en el Registro Central de Rebeldes Civiles, se inscribirán, además, los siguientes datos:

a) Órganos judiciales que hubieran promovido la inscripción o solicitado información sobre la localización de la persona inscrita, así como referencia a los procesos en que aparezca como demandado.

b) Fecha de la resolución en que se acuerde la comunicación mediante edictos al demandado, cuyo domicilio se desconoce y no hayan tenido resultado positivo las averiguaciones practicadas.

Artículo 13. *Inclusión de datos en el sistema.*

1. La trasmisión de datos a los Registros Centrales se realizará a través de procedimientos electrónicos por el secretario judicial que corresponda. A tal efecto, el secretario judicial verificará la exactitud del contenido de la información que, previamente

cumplimentada por el personal de la oficina judicial bajo su dirección, se trasmita a los Registros Centrales. Esta información deberá remitirse en los siguientes plazos:

a) De forma inmediata y, en cualquier caso, en el plazo máximo de cinco días desde la firmeza de la sentencia o auto de rebeldía, desde que se adopte la medida cautelar o sentencia no firme o desde que se acuerde la comunicación edictal cuando se trate de inscripciones en los Registros Centrales de Penados, Medidas Cautelares, Requisitorias y Sentencias No Firmes, Rebeldes Civiles y Sentencias de Responsabilidad Penal de los Menores.

b) De forma inmediata y, en cualquier caso, en el plazo máximo de veinticuatro horas desde la firmeza de la sentencia o desde que se adopte la medida cautelar o sentencia no firme cuando se trate de inscripciones en el Registro Central para la Protección de las Víctimas de Violencia Doméstica. Cuando las circunstancias técnicas impidan la trasmisión telemática a este Registro Central, la trasmisión de datos podrá realizarse mediante la remisión al encargado del registro de los modelos aprobados por Orden del Ministro de Justicia. Los secretarios judiciales ordenarán que se remita en dicho plazo copia impresa de los mismos a la policía judicial a efectos de su ejecución y seguimiento.

2. En cuanto las condiciones técnicas lo permitan, la transmisión de la información se realizará directamente desde las aplicaciones de gestión procesal y las firmas plasmadas en los documentos serán sustituidas por las correspondientes firmas electrónicas reconocidas.

CAPÍTULO IV

Medidas de seguridad

Artículo 14. *Seguridad del sistema.*

1. Se implantarán en el Sistema de registros administrativos de apoyo a la Administración de Justicia las medidas de seguridad que correspondan, de conformidad con el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

De cada intento de acceso se guardará como mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

2. Las redes de comunicación electrónica gestionadas por las comunidades autónomas que den soporte a los órganos judiciales estarán conectadas con el Sistema de Registros Centrales, en un entorno integrado en red, que garantice la confidencialidad y autenticidad de dichas comunicaciones.

Artículo 15. *Seguridad de los datos.*

Se aplicarán a los datos de carácter personal contenidos en el Sistema de registros administrativos de apoyo a la Administración de Justicia las medidas de seguridad que correspondan, de conformidad con el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

CAPÍTULO V

Certificación de los datos

Artículo 16. *Certificación de los datos inscritos en el Sistema de registros administrativos de apoyo a la Administración de Justicia.*

Se emitirán certificaciones de los datos inscritos en el Sistema de registros administrativos de apoyo a la Administración de Justicia en los siguientes casos:

a) Los órganos judiciales, en relación con las causas que tramiten y para su unión al procedimiento, podrán, a través del personal de la oficina judicial autorizado por el Secretario Judicial, obtener directamente los datos incluidos en de las Bases de Datos del Sistema de registros administrativos de apoyo a la Administración de Justicia. Los datos así obtenidos se aportarán al procedimiento judicial mediante diligencia de constancia del Secretario Judicial con plena validez jurídica, sin necesidad de solicitar certificación al Responsable de Registro.

Sin perjuicio de lo anterior, los órganos judiciales podrán recabar del Registro, por vía telemática y de acuerdo con un modelo normalizado, la certificación.

b) Por el Encargado de los Registros integrados en el Sistema de registros administrativos de apoyo a la Administración de Justicia se informará a las autoridades de Estados extranjeros, en las formas y supuestos que determinen las normas comunitarias y los tratados internacionales de asistencia judicial en materia penal suscritos por España, acerca de las sentencia condenatorias firmes impuestas a personas físicas mayores de edad relativas a extranjeros o españoles de las que exista constancia y en su caso, a personas jurídicas y entes sin personalidad.

c) Por el Encargado de los Registros integrados en el Sistema de registros administrativos de apoyo a la Administración de Justicia, siempre que no se trate de información reservada a Jueces y Tribunales, se informará igualmente de los datos contenidos en las inscripciones de los Registros Centrales de Penados, de Medidas Cautelares, Requisitorias y Sentencias No Firmes, de Protección de las Víctimas de Violencia Doméstica y de Rebeldes Civiles, a instancia de cualquier órgano de las Administraciones Públicas ante el que se tramite un procedimiento en el que sea preceptivo este certificado para acceder a un derecho o adquirir una condición determinada con consentimiento del interesado, sea este persona física, jurídica o entes sin personalidad, manifestado directamente o a través de su representante, salvo que una norma con rango de Ley lo exceptúe. Dicha información se limitará únicamente a los datos relativos a la persona física, jurídica o ente sin personalidad interesado en el procedimiento.

Artículo 17. *Certificación a petición del titular interesado.*

1. A petición del titular interesado, podrán certificarse directamente los datos relativos a su persona contenidos en las inscripciones de los Registros Centrales de Penados, de Medidas Cautelares Requisitorias y Sentencias No Firmes, de Protección de las Víctimas de Violencia Doméstica, de Sentencias de Responsabilidad Penal de los Menores y de Rebeldes Civiles y suscribir certificaciones negativas respecto a personas que no figuren inscritas en los mismos.

2. Las certificaciones podrán solicitarse respecto de uno o varios registros integrados en el sistema o respecto de todos ellos. Tratándose de personas jurídicas, entes sin personalidad o menores de edad la solicitud deberá efectuarse, en todo caso, por su representante legal. La certificación positiva contendrá la transcripción de los datos inscritos, tal y como obren en el Registro en el momento de su expedición, excluyendo las inscripciones que, conforme a una norma con rango de Ley, se hallen a disposición únicamente de los órganos jurisdiccionales.

3. Las certificaciones serán entregadas directamente al titular de la información penal o a su representante debidamente acreditado por cualquier medio válido en derecho que deje constancia fidedigna.

4. Los titulares interesados podrán solicitar y recibir por correo el certificado correspondiente a sus datos personales o de la persona jurídica o ente sin personalidad de que se trate; en el caso de personas jurídicas y de los entes sin personalidad, la solicitud habrá de formularse por su representante legal. Mediante Orden del Ministro de Justicia se determinarán los requisitos y condiciones para que dichas solicitudes puedan tramitarse por vía electrónica.

5. Los españoles que se encuentran en el extranjero podrán solicitar el certificado en la oficina consular de España, previa acreditación de su personalidad. Podrán solicitar la remisión del certificado a dicho consulado, por correo al lugar señalado al efecto, o nombrar un representante para recoger la certificación en el Registro Central o en una Gerencia Territorial del Ministerio de Justicia.

6. Cuando se trate de ciudadanos de la Unión Europea con nacionalidad distinta a la española el Registro Central de Penados solicitará a la autoridad central del Estado de nacionalidad de la persona que realiza la petición, o a las autoridades centrales en caso de que la persona tuviera más de una nacionalidad, un extracto de antecedentes penales y de información sobre dichos antecedentes para poder incluirla en el certificado que se le facilite.

7. Las certificaciones a que se refiere este artículo y el apartado c) del artículo anterior no incluirán datos relativos a las inscripciones derivadas de la comisión de faltas.

CAPÍTULO VI

Cancelación o rectificación de inscripciones

Artículo 18. *Normas generales de cancelación o rectificación de inscripciones.*

1. La cancelación de las inscripciones se practicará de oficio, a instancia del titular interesado, o por comunicación del órgano judicial.

Corresponde al Ministerio de Justicia resolver el procedimiento para la cancelación de las inscripciones, cualquiera que sea la forma de iniciación del procedimiento.

2. Los titulares interesados podrán solicitar la cancelación o rectificación de sus datos contenidos en el Sistema de registros administrativos del Ministerio de Justicia de Apoyo a la Administración de Justicia. A estos efectos, dirigirán una solicitud en la que se hará constar, nombre y apellidos, filiación, localidad, provincia, fecha de nacimiento y documento nacional de identidad, NIE o tarjeta de identidad o pasaporte en el caso de extranjeros, todos ellos en vigor, acompañando al modelo de solicitud, original de los documentos anteriores o copia compulsada de los mismos. En el caso de personas jurídicas o entes sin personalidad, nombre y apellidos del representante, documento nacional de identidad, NIE o tarjeta de identidad o pasaporte en el caso de extranjeros, todos ellos en vigor, acompañando al modelo de solicitud, original de los documentos anteriores o copia compulsada de los mismos así como la documentación que acredite su condición de representante legal. En la solicitud deberá hacerse constar de manera obligatoria un domicilio a efectos de notificaciones. Mediante Orden del Ministro de Justicia, se determinarán los requisitos y condiciones para que dichas solicitudes puedan tramitarse por vía telemática.

3. También deberá hacerse constar la causa o causas de la cancelación o rectificación que se solicita, pudiendo aportar cuantos documentos puedan ser determinantes para el fin solicitado.

4. Al expediente iniciado a instancia del interesado se llevarán las inscripciones afectadas y si del análisis de las mismas, o de lo aportado por el solicitante, se dedujera que no se dan los requisitos necesarios para proceder a la cancelación o rectificación, el Ministerio de Justicia denegará motivadamente la petición.

5. El encargado del Registro, de oficio, cuando tenga conocimiento a través de los datos obrantes en el Registro de que se dan los requisitos legalmente establecidos para la cancelación de una inscripción, procederá a elevar propuesta de cancelación.

Cuando se trate de procedimientos penales que hayan dado lugar a inscripciones en los que no se haya comunicado modificación alguna durante los plazos de prescripción establecidos en los artículos 131 y 133 del Código Penal, el encargado del Registro Central se dirigirá al secretario judicial del correspondiente órgano judicial a los efectos de verificar su estado procesal, procediendo a cancelar la inscripción cuando así resulte de la comunicación que este le remita.

Artículo 19. *Cancelación de inscripciones de antecedentes penales.*

1. Las inscripciones de antecedentes penales se cancelarán, de oficio o a instancia del titular de los datos, o por comunicación del órgano judicial, cuando habiéndose extinguido la responsabilidad penal, hubiesen trascurrido, sin delinquir de nuevo los plazos previstos y se hubiesen cumplido los restantes requisitos señalados en el artículo 136 del Código Penal.

2. Cuando el procedimiento se inicie de oficio o a instancia del interesado y no constara el informe del Juzgado o Tribunal en relación con el cumplimiento de los requisitos establecidos en el artículo 136 del Código Penal, el Registro de Penados remitirá el expediente en el plazo de quince días a fin de que informe preceptivamente en el plazo

máximo de dos meses sobre la cancelación solicitada. El plazo máximo para resolver y notificar el procedimiento será de tres meses.

3. La información relativa a las inscripciones canceladas se conservará en una sección especial y separada a disposición únicamente de los Juzgados y Tribunales españoles.

Artículo 20. *Cómputo del plazo de cancelación de inscripciones de penas suspendidas.*

Cuando la cancelación de las inscripciones de antecedentes penales se refiera a penas privativas de libertad suspendidas por habérseles aplicado la remisión condicional, el plazo de cancelación, una vez obtenida la remisión definitiva, se computará en la forma establecida en el artículo 136.3 del Código Penal.

Artículo 21. *Pluralidad de antecedentes penales.*

Cuando se inicie un expediente de cancelación de antecedentes penales de oficio o a instancia de parte, y deba cursarse a varios Juzgados o Tribunales, se remitirá el original al que hubiera dictado la última sentencia y copias autenticadas a cada uno de los restantes, debiendo constar en el oficio de remisión el listado de Juzgados o Tribunales a los que se solicita información.

Artículo 22. *Cancelación de inscripciones de medidas cautelares, ordenes de protección, ordenes de busca, Sentencias No Firmes y autos de rebeldía penal.*

1. La cancelación se producirá con carácter automático cuando se produzca la comunicación judicial en la que se exprese el cese de su vigencia.

2. También se cancelarán las inscripciones de medidas cautelares, órdenes de protección y Sentencias No Firmes relativas a un procedimiento en tramitación cuando se proceda a la inscripción de una sentencia firme recaída en el mismo procedimiento.

3. Asimismo, la acumulación de un procedimiento o la inhibición en favor de otro juzgado, producirán la cancelación de las correspondientes anotaciones cuando el encargado del Registro verifique la inscripción de la medida cautelar, orden de protección, orden de busca o auto de rebeldía penal en el procedimiento resultante de la acumulación o la inhibición.

Artículo 23. *Cancelación de las inscripciones de rebeldes civiles.*

1. Procederá la cancelación de la inscripción del rebelde civil a instancia del interesado. También podrá el interesado dirigirse al órgano judicial remitente de la comunicación originaria para que sea el órgano judicial el que se dirija al Registro solicitando la cancelación de la inscripción en cuestión. En la solicitud deberá indicar el domicilio al que se puedan dirigir las comunicaciones judiciales.

2. Cuando se acuerde la cancelación, el Registro deberá comunicar el nuevo domicilio a los órganos judiciales que aparecieran anotados junto a la inscripción.

3. En el caso de que se deniegue la cancelación instada por el interesado por existir dudas racionales sobre la exactitud del domicilio facilitado, el Registro deberá indicarle los defectos que haya apreciado y recordarle la posibilidad de instar nuevamente esa cancelación en cuanto hayan quedado subsanados.

Artículo 24. *Cancelación de las inscripciones del Registro Central de Sentencias sobre Responsabilidad Penal de los Menores.*

Trascurridos diez años, a contar desde que el menor hubiera alcanzado la mayoría de edad y siempre que las medidas judicialmente impuestas hayan sido ejecutadas en su plenitud o hayan prescrito, el Ministerio de Justicia procederá de oficio a la cancelación de cuantas inscripciones de sentencias referentes al mismo consten en el Registro.

Artículo 25. *Efectos de la cancelación.*

La cancelación registral prevista en este real decreto dará lugar a la eliminación de los datos de carácter personal, sin perjuicio de lo dispuesto en el artículo 19.3 del presente real

Decreto y a excepción de aquellos que resulten necesarios para que sea posible elaborar las estadísticas previstas en su artículo 27.

Artículo 26. *Tutela de derechos.*

De conformidad con lo dispuesto en el artículo 18.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los interesados podrán recabar la tutela de la Agencia Española de Protección de Datos en relación con el ejercicio de sus derechos de acceso, rectificación o cancelación.

Artículo 27. *Información estadística.*

La Administración General del Estado y las comunidades autónomas con competencias en materia de justicia, en el marco del Plan de Transparencia Judicial, podrán elaborar estadísticas de los datos contenidos en los Registros Centrales, eludiendo toda referencia personal en la información y teniendo en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos y sus disposiciones complementarias. En particular, el Registro para la Protección de las Victimas de Violencia Doméstica proporcionará a la Delegación de Gobierno para la Violencia de Género la información necesaria para permitir el adecuado conocimiento, análisis y evaluación de la violencia de género, con excepción de los datos de carácter personal de los intervinientes en los procedimientos judiciales. Los datos estadísticos deberán seguir los criterios que establezca la Comisión Nacional de Estadística Judicial.

Disposición adicional primera. *Comunicación de las órdenes de protección a las Administraciones públicas competentes en materia de protección social.*

1. Los secretarios de los juzgados y tribunales comunicarán las órdenes de protección de las víctimas de violencia doméstica que se adopten y sus respectivas solicitudes, mediante testimonio íntegro, a aquel o aquellos puntos de coordinación designados por la comunidad autónoma correspondiente, que constituirán el canal único de notificación de estas resoluciones a centros, unidades, organismos e instituciones competentes en materia de protección social en relación con estas víctimas, de acuerdo con lo establecido en el apartado 8 del articulo 544 ter de la Ley de Enjuiciamiento Criminal.

La comunicación del secretario judicial se remitirá en un plazo nunca superior a 24 horas desde su adopción, por vía telemática o electrónica o, en su defecto, por medio de fax o correo urgente.

2. El punto de coordinación designado hará referencia al centro, unidad, organismo o institución que centraliza la información, su dirección postal y electrónica, números de teléfono y fax, régimen horario y persona o personas responsables de aquél. En el caso de comunidades autónomas pluriprovinciales, podrá identificarse un punto de conexión específico para cada provincia.

3. El Consejo General del Poder Judicial mantendrá una relación actualizada de los puntos de coordinación designados, remitirá tal identificación en su integridad y sus modificaciones o actualizaciones a los Ministerios de Justicia, de Igualdad y del Interior, así como a la Fiscalía General del Estado y al Tribunal Superior de Justicia, decanatos y juzgados de instrucción del ámbito autonómico correspondiente.

Disposición adicional segunda. *Prestación de consentimiento.*

A efectos de lo dispuesto en los artículos 6.b) y c) y 7.1.b) y c) del presente real decreto, el acceso de las Unidades de Intervención de Armas y Explosivos de la Guardia Civil y de las Unidades del Cuerpo Nacional de Policía responsables de la expedición del pasaporte, a la información contenida en las Bases de Datos del Sistema de registros administrativos de apoyo a la Administración de Justicia, requerirá el previo consentimiento del interesado, quien podrá manifestarlo en la propia solicitud.

Disposición adicional tercera. *Jurisdicción militar.*

Los órganos de la Jurisdicción Militar estarán sujetos a lo dispuesto en la presente norma salvo en lo que no les sea de aplicación.

Disposición adicional cuarta. *Fondo documental de requisitorias.*

1. Se crea en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes y en el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, el Fondo Documental de Requisitorias.
2. El Fondo Documental de Requisitorias estará formado por todos los testimonios de las resoluciones judiciales y de particulares correspondientes, de acuerdo con el artículo 516 de la Ley de Enjuiciamiento Criminal.
3. Para formar el fondo documental de requisitorias, será suficiente la digitalización material de los testimonios y su inclusión en el sistema informático, garantizando su autenticidad, integridad y conservación del documento imagen, conforme lo previsto en los apartados 2 y 3 del artículo 28 de la Ley 18/2011, de 5 julio, reguladora del uso de las tecnologías de la comunicación y la información en la Administración de Justicia.
4. La documentación asociada a cada requisitoria inscrita en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes o en el Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, a partir de la entrada en vigor del presente Real Decreto estará disponible únicamente para los órganos judiciales y el Ministerio Fiscal, y exclusivamente a los efectos de los procedimientos y actuaciones de los que estén conociendo, en el ámbito de sus respectivas competencias. Dicho acceso se llevará a cabo por el personal de la oficina judicial autorizado por el Secretario del Órgano Judicial del que emana la requisitoria.
5. Los documentos asociados a cada requisitoria quedarán automáticamente eliminados cuando se produzca la cancelación de la requisitoria.

Disposición transitoria primera. *Comunicaciones anteriores a la entrada en vigor del real decreto.*

Las comunicaciones que los órganos judiciales hayan dirigido al Ministerio de Justicia antes de la entrada en vigor del presente real decreto, se regirán por la normativa anterior, si la hubiese.

Disposición transitoria segunda. *Inscripción de medidas cautelares personales, requisitorias y Sentencias No Firmes acordadas con anterioridad a la entrada en vigor del presente real decreto.*

Las medidas cautelares de carácter personal y las requisitorias y las Sentencias No Firmes acordadas o dictadas con anterioridad a la entrada en vigor del presente real decreto y que se encuentren en vigor, deberán inscribirse en el Registro Central de Medidas Cautelares, Requisitorias y Sentencias no Firmes.

Estas inscripciones deberán efectuarse en el plazo de tres meses desde la entrada en vigor del presente real decreto.

Disposición transitoria tercera. *Inscripción de penas derivadas de la comisión de una falta en los Registros de Penados y Rebeldes y Medidas Cautelares, Requisitorias y Sentencias no Firmes.*

La inscripción de resoluciones firmes en los Registros de Penados y Rebeldes y Medidas Cautelares, Requisitorias y Sentencias No Firmes por la comisión de una falta, se producirá a partir del momento en que se encuentre en funcionamiento el sistema de envío automático de datos previsto en el artículo 13.2 del presente real decreto.

Disposición derogatoria única. *Derogación normativa.*

Quedan expresamente derogados el Real Decreto de 2 de Octubre de 1878, la Real Orden de 1 de Abril de 1896, el Real Decreto 2012/1983, de 28 de Julio, sobre cancelación de antecedentes penales, Real Decreto 231/2002, de 1 de marzo, por el que se regula el

Registro Central de Rebeldes Civiles, el Real Decreto 232/2002, de 1 de marzo, por el que se regula el Registro de Sentencias Firmes sobre Responsabilidad Penal de los Menores, el Real Decreto 355/2004, de 5 de marzo, por el que se regula el Registro Central para la protección de las víctimas de la violencia doméstica y cuantas disposiciones contenidas en normas de igual o inferior rango al presente real decreto se opongan a lo previsto en él.

Disposición final primera. *Título competencial.*

El presente real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.5 de la Constitución, que atribuye al Estado la competencia exclusiva en materia de Administración de Justicia.

Disposición final segunda. *Facultades de desarrollo.*

Se autoriza al Ministro de Justicia a dictar cuantas disposiciones sean necesarias para el desarrollo de la presente norma.

Disposición final tercera. *Alimentación automática de la información contenida en el Sistema.*

El Ministerio de Justicia y las comunidades autónomas con traspasos recibidos en materia de Justicia deberán realizar las modificaciones oportunas en los respectivos sistemas de gestión procesal para que la transmisión de la información prevista en el artículo 13.2 del presente real decreto tenga lugar en el plazo máximo de dieciocho meses, a partir de la entrada en vigor del presente real decreto.

Disposición final cuarta. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

INFORMACION RELACIONADA:
- Las referencias hechas al Registro Central para la Protección de las Víctimas de Violencia Doméstica se entenderán efectuadas al Registro Central para la Protección de las Víctimas de la Violencia Doméstica y de Género, conforme a lo dispuesto en la disposición adicional única del Real Decreto 1611/2011, de 14 de noviembre. Ref. BOE-A-2011-18912.

§ 24

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 10 de julio de 2021
Referencia: BOE-A-2015-10565

[. . .]

TÍTULO II

De la actividad de las Administraciones Públicas

CAPÍTULO I

Normas generales de actuación

Artículo 13. *Derechos de las personas en sus relaciones con las Administraciones Públicas.*

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.

b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.

c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.

d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.

e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.

f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.

g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.

h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

Artículo 14. *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento.

2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica.

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.

d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.

e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración.

3. Reglamentariamente, las Administraciones podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

[. . .]

TÍTULO III

De los actos administrativos

[. . .]

CAPÍTULO II

Eficacia de los actos

[. . .]

Artículo 40. *Notificación.*

1. El órgano que dicte las resoluciones y actos administrativos los notificará a los interesados cuyos derechos e intereses sean afectados por aquéllos, en los términos previstos en los artículos siguientes.

2. Toda notificación deberá ser cursada dentro del plazo de diez días a partir de la fecha en que el acto haya sido dictado, y deberá contener el texto íntegro de la resolución, con indicación de si pone fin o no a la vía administrativa, la expresión de los recursos que procedan, en su caso, en vía administrativa y judicial, el órgano ante el que hubieran de presentarse y el plazo para interponerlos, sin perjuicio de que los interesados puedan ejercitar, en su caso, cualquier otro que estimen procedente.

3. Las notificaciones que, conteniendo el texto íntegro del acto, omitiesen alguno de los demás requisitos previstos en el apartado anterior, surtirán efecto a partir de la fecha en que

el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación, o interponga cualquier recurso que proceda.

4. Sin perjuicio de lo establecido en el apartado anterior, y a los solos efectos de entender cumplida la obligación de notificar dentro del plazo máximo de duración de los procedimientos, será suficiente la notificación que contenga, cuando menos, el texto íntegro de la resolución, así como el intento de notificación debidamente acreditado.

5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la protección de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado.

Artículo 41. *Condiciones generales para la práctica de las notificaciones.*

1. Las notificaciones se practicarán preferentemente por medios electrónicos y, en todo caso, cuando el interesado resulte obligado a recibirlas por esta vía.

No obstante lo anterior, las Administraciones podrán practicar las notificaciones por medios no electrónicos en los siguientes supuestos:

a) Cuando la notificación se realice con ocasión de la comparecencia espontánea del interesado o su representante en las oficinas de asistencia en materia de registro y solicite la comunicación o notificación personal en ese momento.

b) Cuando para asegurar la eficacia de la actuación administrativa resulte necesario practicar la notificación por entrega directa de un empleado público de la Administración notificante.

Con independencia del medio utilizado, las notificaciones serán válidas siempre que permitan tener constancia de su envío o puesta a disposición, de la recepción o acceso por el interesado o su representante, de sus fechas y horas, del contenido íntegro, y de la identidad fidedigna del remitente y destinatario de la misma. La acreditación de la notificación efectuada se incorporará al expediente.

Los interesados que no estén obligados a recibir notificaciones electrónicas, podrán decidir y comunicar en cualquier momento a la Administración Pública, mediante los modelos normalizados que se establezcan al efecto, que las notificaciones sucesivas se practiquen o dejen de practicarse por medios electrónicos.

Reglamentariamente, las Administraciones podrán establecer la obligación de practicar electrónicamente las notificaciones para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

Adicionalmente, el interesado podrá identificar un dispositivo electrónico y/o una dirección de correo electrónico que servirán para el envío de los avisos regulados en este artículo, pero no para la práctica de notificaciones.

2. En ningún caso se efectuarán por medios electrónicos las siguientes notificaciones:

a) Aquellas en las que el acto a notificar vaya acompañado de elementos que no sean susceptibles de conversión en formato electrónico.

b) Las que contengan medios de pago a favor de los obligados, tales como cheques.

3. En los procedimientos iniciados a solicitud del interesado, la notificación se practicará por el medio señalado al efecto por aquel. Esta notificación será electrónica en los casos en los que exista obligación de relacionarse de esta forma con la Administración.

Cuando no fuera posible realizar la notificación de acuerdo con lo señalado en la solicitud, se practicará en cualquier lugar adecuado a tal fin, y por cualquier medio que permita tener constancia de la recepción por el interesado o su representante, así como de la fecha, la identidad y el contenido del acto notificado.

4. En los procedimientos iniciados de oficio, a los solos efectos de su iniciación, las Administraciones Públicas podrán recabar, mediante consulta a las bases de datos del Instituto Nacional de Estadística, los datos sobre el domicilio del interesado recogidos en el Padrón Municipal, remitidos por las Entidades Locales en aplicación de lo previsto en la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

5. Cuando el interesado o su representante rechace la notificación de una actuación administrativa, se hará constar en el expediente, especificándose las circunstancias del intento de notificación y el medio, dando por efectuado el trámite y siguiéndose el procedimiento.

6. Con independencia de que la notificación se realice en papel o por medios electrónicos, las Administraciones Públicas enviarán un aviso al dispositivo electrónico y/o a la dirección de correo electrónico del interesado que éste haya comunicado, informándole de la puesta a disposición de una notificación en la sede electrónica de la Administración u Organismo correspondiente o en la dirección electrónica habilitada única. La falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

7. Cuando el interesado fuera notificado por distintos cauces, se tomará como fecha de notificación la de aquélla que se hubiera producido en primer lugar.

Artículo 42. *Práctica de las notificaciones en papel.*

1. Todas las notificaciones que se practiquen en papel deberán ser puestas a disposición del interesado en la sede electrónica de la Administración u Organismo actuante para que pueda acceder al contenido de las mismas de forma voluntaria.

2. Cuando la notificación se practique en el domicilio del interesado, de no hallarse presente éste en el momento de entregarse la notificación, podrá hacerse cargo de la misma cualquier persona mayor de catorce años que se encuentre en el domicilio y haga constar su identidad. Si nadie se hiciera cargo de la notificación, se hará constar esta circunstancia en el expediente, junto con el día y la hora en que se intentó la notificación, intento que se repetirá por una sola vez y en una hora distinta dentro de los tres días siguientes. En caso de que el primer intento de notificación se haya realizado antes de las quince horas, el segundo intento deberá realizarse después de las quince horas y viceversa, dejando en todo caso al menos un margen de diferencia de tres horas entre ambos intentos de notificación. Si el segundo intento también resultara infructuoso, se procederá en la forma prevista en el artículo 44.

3. Cuando el interesado accediera al contenido de la notificación en sede electrónica, se le ofrecerá la posibilidad de que el resto de notificaciones se puedan realizar a través de medios electrónicos.

Artículo 43. *Práctica de las notificaciones a través de medios electrónicos.*

1. Las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica de la Administración u Organismo actuante, a través de la dirección electrónica habilitada única o mediante ambos sistemas, según disponga cada Administración u Organismo.

A los efectos previstos en este artículo, se entiende por comparecencia en la sede electrónica, el acceso por el interesado o su representante debidamente identificado al contenido de la notificación.

2. Las notificaciones por medios electrónicos se entenderán practicadas en el momento en que se produzca el acceso a su contenido.

Cuando la notificación por medios electrónicos sea de carácter obligatorio, o haya sido expresamente elegida por el interesado, se entenderá rechazada cuando hayan transcurrido diez días naturales desde la puesta a disposición de la notificación sin que se acceda a su contenido.

3. Se entenderá cumplida la obligación a la que se refiere el artículo 40.4 con la puesta a disposición de la notificación en la sede electrónica de la Administración u Organismo actuante o en la dirección electrónica habilitada única.

4. Los interesados podrán acceder a las notificaciones desde el Punto de Acceso General electrónico de la Administración, que funcionará como un portal de acceso.

Artículo 44. *Notificación infructuosa.*

Cuando los interesados en un procedimiento sean desconocidos, se ignore el lugar de la notificación o bien, intentada ésta, no se hubiese podido practicar, la notificación se hará por medio de un anuncio publicado en el «Boletín Oficial del Estado».

Asimismo, previamente y con carácter facultativo, las Administraciones podrán publicar un anuncio en el boletín oficial de la Comunidad Autónoma o de la Provincia, en el tablón de edictos del Ayuntamiento del último domicilio del interesado o del Consulado o Sección Consular de la Embajada correspondiente.

Las Administraciones Públicas podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión, que no excluirán la obligación de publicar el correspondiente anuncio en el «Boletín Oficial del Estado».

Artículo 45. *Publicación.*

1. Los actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente.

En todo caso, los actos administrativos serán objeto de publicación, surtiendo ésta los efectos de la notificación, en los siguientes casos:

a) Cuando el acto tenga por destinatario a una pluralidad indeterminada de personas o cuando la Administración estime que la notificación efectuada a un solo interesado es insuficiente para garantizar la notificación a todos, siendo, en este último caso, adicional a la individualmente realizada.

b) Cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo. En este caso, la convocatoria del procedimiento deberá indicar el medio donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos.

2. La publicación de un acto deberá contener los mismos elementos que el artículo 40.2 exige respecto de las notificaciones. Será también aplicable a la publicación lo establecido en el apartado 3 del mismo artículo.

En los supuestos de publicaciones de actos que contengan elementos comunes, podrán publicarse de forma conjunta los aspectos coincidentes, especificándose solamente los aspectos individuales de cada acto.

3. La publicación de los actos se realizará en el diario oficial que corresponda, según cual sea la Administración de la que proceda el acto a notificar.

4. Sin perjuicio de lo dispuesto en el artículo 44, la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deba practicarse en tablón de anuncios o edictos, se entenderá cumplida por su publicación en el Diario oficial correspondiente.

Artículo 46. *Indicación de notificaciones y publicaciones.*

Si el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos, se limitará a publicar en el Diario oficial que corresponda una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para conocimiento del contenido íntegro del mencionado acto y constancia de tal conocimiento.

Adicionalmente y de manera facultativa, las Administraciones podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión que no excluirán la obligación de publicar en el correspondiente Diario oficial.

CAPÍTULO III

Nulidad y anulabilidad

Artículo 47. *Nulidad de pleno derecho.*

1. Los actos de las Administraciones Públicas son nulos de pleno derecho en los casos siguientes:

a) Los que lesionen los derechos y libertades susceptibles de amparo constitucional.

b) Los dictados por órgano manifiestamente incompetente por razón de la materia o del territorio.

c) Los que tengan un contenido imposible.

d) Los que sean constitutivos de infracción penal o se dicten como consecuencia de ésta.

e) Los dictados prescindiendo total y absolutamente del procedimiento legalmente establecido o de las normas que contienen las reglas esenciales para la formación de la voluntad de los órganos colegiados.

f) Los actos expresos o presuntos contrarios al ordenamiento jurídico por los que se adquieren facultades o derechos cuando se carezca de los requisitos esenciales para su adquisición.

g) Cualquier otro que se establezca expresamente en una disposición con rango de Ley.

2. También serán nulas de pleno derecho las disposiciones administrativas que vulneren la Constitución, las leyes u otras disposiciones administrativas de rango superior, las que regulen materias reservadas a la Ley, y las que establezcan la retroactividad de disposiciones sancionadoras no favorables o restrictivas de derechos individuales.

Artículo 48. *Anulabilidad.*

1. Son anulables los actos de la Administración que incurran en cualquier infracción del ordenamiento jurídico, incluso la desviación de poder.

2. No obstante, el defecto de forma sólo determinará la anulabilidad cuando el acto carezca de los requisitos formales indispensables para alcanzar su fin o dé lugar a la indefensión de los interesados.

3. La realización de actuaciones administrativas fuera del tiempo establecido para ellas sólo implicará la anulabilidad del acto cuando así lo imponga la naturaleza del término o plazo.

Artículo 49. *Límites a la extensión de la nulidad o anulabilidad de los actos.*

1. La nulidad o anulabilidad de un acto no implicará la de los sucesivos en el procedimiento que sean independientes del primero.

2. La nulidad o anulabilidad en parte del acto administrativo no implicará la de las partes del mismo independientes de aquélla, salvo que la parte viciada sea de tal importancia que sin ella el acto administrativo no hubiera sido dictado.

Artículo 50. *Conversión de actos viciados.*

Los actos nulos o anulables que, sin embargo, contengan los elementos constitutivos de otro distinto producirán los efectos de éste.

Artículo 51. *Conservación de actos y trámites.*

El órgano que declare la nulidad o anule las actuaciones dispondrá siempre la conservación de aquellos actos y trámites cuyo contenido se hubiera mantenido igual de no haberse cometido la infracción.

Artículo 52. *Convalidación.*

1. La Administración podrá convalidar los actos anulables, subsanando los vicios de que adolezcan.

2. El acto de convalidación producirá efecto desde su fecha, salvo lo dispuesto en el artículo 39.3 para la retroactividad de los actos administrativos.

3. Si el vicio consistiera en incompetencia no determinante de nulidad, la convalidación podrá realizarse por el órgano competente cuando sea superior jerárquico del que dictó el acto viciado.

4. Si el vicio consistiese en la falta de alguna autorización, podrá ser convalidado el acto mediante el otorgamiento de la misma por el órgano competente.

[. . .]

§ 25

Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. [Inclusión parcial]

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 77, de 31 de marzo de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-5032

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, consagran el derecho de las personas a relacionarse por medios electrónicos con las administraciones públicas, simplificando el acceso a los mismos, y refuerzan el empleo de las tecnologías de la información y las comunicaciones (TIC) en las administraciones públicas, tanto para mejorar la eficiencia de su gestión como para potenciar y favorecer las relaciones de colaboración y cooperación entre ellas.

Ambas leyes recogen los elementos que conforman el marco jurídico para el funcionamiento electrónico de las Administraciones Públicas introduciendo un nuevo paradigma que supera la concepción que inspiró la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su desarrollo reglamentario parcial en la Administración General del Estado y sus organismos públicos vinculados o dependientes a través del Real Decreto 1671/2009, de 6 de noviembre, según la cual la tramitación electrónica no era sino una forma de gestión de los procedimientos.

En este sentido, la Ley 11/2007, de 22 de junio, respondiendo a las nuevas realidades, exigencias y experiencias que se habían puesto de manifiesto, al propio desarrollo de la sociedad de la información y al cambio de circunstancias tecnológicas y sociales, entre otros factores, reconocía el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas, y no solo la posibilidad como se preveía en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La Ley 11/2007, de 22 de junio admitía incluso que, por vía reglamentaria, se estableciese la obligatoriedad de comunicarse con las Administraciones Públicas por medios electrónicos cuando las personas interesadas fuesen personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tuviesen garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

En este contexto, la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, han dado respuesta a la demanda actual en el sentido de que la tramitación electrónica de los procedimientos debe constituir la actuación habitual de las Administraciones Públicas, y no solamente ser una forma especial de gestión de los mismos. En consecuencia, se prevé que las relaciones de las Administraciones entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes se realizará a través de medios electrónicos, y se

establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, entes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria.

Con estos antecedentes, era necesario desarrollar y concretar las previsiones legales con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria.

La satisfacción del interesado, por tanto, en el uso de los servicios públicos digitales es fundamental para garantizar adecuadamente sus derechos y el cumplimiento de sus obligaciones en su relación con las Administraciones Públicas. Por ello, es prioritario disponer de servicios digitales fácilmente utilizables y accesibles, de modo que se pueda conseguir que la relación del interesado con la Administración a través del canal electrónico sea fácil, intuitiva, efectiva, eficiente y no discriminatoria.

Por otra parte, a lo largo de las dos últimas décadas, los sucesivos Gobiernos de España han ido adoptando programas para el avance digital alineados con las agendas digitales europeas, en todos los cuales ha estado presente el eje de mejora de la Administración electrónica. Fruto de estos programas, España cuenta con una posición muy favorable para abordar la siguiente fase del proceso de Transformación digital de nuestro país y, en lo que concierne a la Administración electrónica, está situada entre los países más avanzados de la Unión Europea, lo que se ha logrado gracias al esfuerzo continuado de las Administraciones Públicas en la adaptación de sus servicios electrónicos para ofrecer cada vez mejores servicios, más adaptados a las demandas de la ciudadanía y las empresas, y más eficientes. En este esfuerzo, la estrategia de España se ha basado en el impulso de los fundamentos que permiten una tramitación electrónica completa, y en el desarrollo de servicios que pueden ser utilizados libremente por todas las Administraciones Públicas, y que están alineados con los esquemas de interoperabilidad europeos.

Los cambios que se están produciendo con la maduración de tecnologías disruptivas y su aplicación a la gestión de la información y la ejecución de políticas públicas, los nuevos modelos de relación de la ciudadanía y empresas con las Administraciones y la reutilización eficiente de la información son grandes desafíos que para ser afrontados con éxito y para que coadyuven a la Transformación digital exigen como presupuesto contar con un marco regulatorio adecuado, tanto con rango de ley como con rango reglamentario, que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables.

En este sentido, la Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y específicamente en la aprobación de este real decreto. Por su parte, el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos, que actúe como tractor de los cambios tecnológicos. El último hito en estrategia transformadora lo constituye el Plan de Digitalización de las Administraciones Públicas 2021 -2025, que supone un salto decisivo en la mejora de la eficacia y eficiencia de la Administración Pública, en la transparencia y eliminación de trabas administrativas a través de la automatización de la gestión, en una mayor orientación a la personalización de servicios y a la experiencia de usuario, actuando todo ello de elemento catalizador de la innovación tecnológica de nuestro país desde el ámbito público.

En definitiva, el Reglamento que aprueba este real decreto persigue los cuatro grandes objetivos mencionados: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

En primer lugar, persigue mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada. Así, se desarrolla y concreta el empleo de los medios electrónicos establecidos en las leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, para garantizar, por una parte, que los procedimientos administrativos se tramiten electrónicamente por la Administración y, por otra, que la ciudadanía se relacione con ella por estos medios en los supuestos en que sea establecido con carácter obligatorio o aquellos lo decidan voluntariamente.

Un segundo objetivo consiste en incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica. Así, se desarrolla el funcionamiento del Punto de Acceso General electrónico (PAGe), y la Carpeta ciudadana en el Sector Público Estatal. Se regula el contenido y los servicios mínimos a prestar por las sedes electrónicas y sedes electrónicas asociadas y el funcionamiento de los registros electrónicos.

En tercer lugar, el Reglamento persigue garantizar servicios digitales fácilmente utilizables de modo que se pueda conseguir que la relación del interesado con la Administración sea fácil, intuitiva y efectiva cuando use el canal electrónico.

Por último, busca mejorar la seguridad jurídica. Así, se elimina la superposición de regímenes jurídicos distintos, se adapta e integra en el Reglamento que aprueba este real decreto la regulación que aún permanecía vigente del Real Decreto 1671/2009, de 6 de noviembre, procediendo, por ello, a su derogación definitiva y se adecua la regulación al nuevo marco de la Ley 39/2015, de 1 de octubre y la Ley 40/2015, de 1 de octubre.

El real decreto consta de un artículo único que aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, dos disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

Entre las cinco disposiciones finales hay dos que modifican normas vigentes y las tres restantes regulan el título competencial, la habilitación reglamentaria para el desarrollo y ejecución del real decreto y la entrada en vigor. Respecto de las disposiciones modificativas, estas afectan al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y al Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Así, en primer lugar, con relación al Real Decreto 4/2010, de 8 de enero, su artículo 29 establece que el Esquema Nacional de Interoperabilidad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Por ello, la rápida evolución de las tecnologías, la experiencia derivada de la aplicación del Esquema Nacional de Interoperabilidad desde su aprobación hace 10 años, las previsiones de la Ley 39/2015, de 1 de octubre, y de la Ley 40/2015, de 1 de octubre, relativas a la interoperabilidad entre las Administraciones Públicas y sus órganos, organismos públicos y entidades de derecho público vinculados o dependientes, más la necesidad de adecuarse a lo previsto en el Reglamento n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/2006/CE del Parlamento Europeo y del Consejo, determinan la necesidad de proceder a modificar ciertos aspectos de su redacción actual. En consecuencia, se modifican los artículos, 9, 11, 14, 16, 17, y 18, así como la disposición adicional primera y el anexo de glosario, a la vez que se suprimen el artículo 19 y las disposiciones adicionales tercera y cuarta.

En segundo lugar, se modifica el Real Decreto 931/2017, de 27 de octubre, para incorporar en la Memoria del Análisis de Impacto Normativo el análisis de la incidencia en los gastos en medios o servicios de la Administración digital dentro del impacto presupuestario de los proyectos y, por otra parte, para incluir dentro del apartado de «Otros impactos» el que tendrá para las personas destinatarias de la norma y para la organización y funcionamiento de la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la aplicación de la normativa proyectada.

Por su parte, el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos que aprueba el real decreto consta de 65 artículos distribuidos en cuatro títulos, diez disposiciones adicionales y un anexo de definiciones.

El título preliminar del Reglamento comprende las disposiciones generales regulando el objeto y ámbito de aplicación de la norma (que se remite al ámbito del artículo 2 tanto de la Ley 39/2015, de 1 de octubre, como de la Ley 40/2015, de 1 de octubre) y los principios generales que debe respetar el sector público en sus actuaciones y relaciones electrónicas. Entre estos principios se incluyen el de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado; el principio de accesibilidad, para promover que el diseño de los servicios electrónicos garantice la igualdad y no discriminación en el acceso de las personas usuarias, en particular, de las personas discapacitadas y de las personas mayores; el principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias para minimizar el grado de conocimiento tecnológico necesario para el uso del servicio, el principio de interoperabilidad, entendido como la capacidad de los sistemas de información y,por ende, de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos; el principio de proporcionalidad, para que las medidas de seguridad y garantías que se exijan sean adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos y, por último, el principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Asimismo el título preliminar regula el derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas, en aplicación del artículo 14 de la Ley 39/2015, de 1 de octubre, y los canales a través de los cuales las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito.

El título I regula los portales de internet, el PAGe, las sedes electrónicas y sedes electrónicas asociadas (características, creación y supresión, contenido y servicios, y responsabilidad) y el área personalizada a través de la cual cada interesado podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente, que en el ámbito estatal se denomina «Carpeta Ciudadana».

El título II se subdivide en tres capítulos y regula el procedimiento administrativo por medios electrónicos. Así, el capítulo I, sobre «Disposiciones generales» aborda la tramitación administrativa automatizada y el régimen de subsanaciones. Por su parte el capítulo II regula la identificación y autenticación de las Administraciones Públicas y de las personas interesadas y se subdivide en cuatro Secciones: la 1ª aborda las disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad (incluyendo la plataforma de verificación de certificados electrónicos y otros sistemas de identificación), la 2.ª regula la «Identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia», que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional) y la autenticación e identificación de las Administraciones emisoras y receptoras en intercambio de datos a través de entornos cerrados de comunicación. La sección 3ª desarrolla la regulación de la identificación y firma de las personas interesadas y, por último, la sección 4ª regula la acreditación de la representación de las personas interesadas (regulando, entre otros extremos, el registro electrónico de apoderamientos).

El título II se cierra con el capítulo III, que en sus dos secciones regula los Registros electrónicos, las notificaciones electrónicas y los otros actos de comunicación electrónicos.

Así, la sección 1ª regula los registros electrónicos (entre otros aspectos, el Registro Electrónico General de cada Administración y la presentación y tratamiento de documentos en registro o las competencias de las Oficinas de asistencia en materia de registros de la Administración General del Estado) y la sección 2ª regula las comunicaciones administrativas a las personas interesadas por medios electrónicos (actos de comunicación electrónica a las personas interesadas distintos de las notificaciones o publicaciones) y las notificaciones electrónicas (incluyendo las reglas generales de la práctica de las notificaciones electrónicas, el aviso de puesta a disposición de la notificación, la notificación a través de la Dirección Electrónica Habilitada única (DEHu) y la notificación electrónica en sede electrónica o sede electrónica asociada).

El título III regula el expediente electrónico y se divide en dos capítulos. El capítulo I regula el documento administrativo electrónico y los requisitos y la emisión de copias auténticas de documentos públicos administrativos o documentos privados, que sean originales o copias auténticas de originales; la formación del expediente administrativo electrónico y el ejercicio de acceso al mismo y a la obtención de copias y la destrucción de documentos. Por su parte, el capítulo II regula la conservación de documentos electrónicos y la definición de archivo electrónico único.

Por último, el título IV se divide en dos capítulos y regula las relaciones y colaboración entre Administraciones Públicas para el funcionamiento electrónico del sector público. Así, el capítulo I aborda la colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos e incluye las obligadas relaciones interadministrativas e interorgánicas por medios electrónicos en el ejercicio de sus competencias, las comunicaciones en la Administración General del Estado, la posibilidad de adhesión a sedes electrónicas y sedes electrónicas asociadas y la regulación del Sistema de Interconexión de Registros (SIR), a través del cual deberán realizarse las interconexiones entre Registros de las Administraciones Públicas, que deberán ser interoperables entre sí y, en el caso de la Administración General del Estado, lo que supone una novedad, también con los sistemas de gestión de expedientes.

El capítulo I del título IV regula también las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015 de 1 de octubre, las plataformas de intermediación de datos (con mención especial a la de ámbito estatal), la remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico completo y, por último, las previsiones el intercambio automático de datos o documentos a nivel europeo previstos en el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012.

El título IV finaliza con el capítulo II, que regula la transferencia y uso compartido de tecnologías entre Administraciones Públicas, abordando, por una parte, la reutilización de sistemas y aplicaciones de las Administraciones Públicas y, por otra, la adhesión a las plataformas, registros o servicios electrónicos de la Administración General del Estado

La parte final del Reglamento consta de diez disposiciones adicionales y un anexo de definiciones. Las primeras regulan la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado; la promoción de la formación del personal al servicio de la Administración General del Estado para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública; la creación del nodo de interoperabilidad para la identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre Estados miembros de la Unión Europea; la adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado, en el ejercicio de potestades administrativas, a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables; la adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado; la situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a

la entrada en vigor de este real decreto; la interoperabilidad de los registros electrónicos de apoderamientos; supletoriedad en Registro Civil; la autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre y, por último, las especialidades por razón de materia.

El Reglamento concluye con un Anexo terminológico que retoma la buena praxis que incluía la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en una materia de especial complejidad por la imbricación de categorías jurídicas y conceptos tecnológicos en permanente evolución.

El real decreto se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia), en tanto que persigue un interés general al concretar determinados aspectos de la Ley 39/2015, de 1 de octubre y de la Ley 40/2015, de 1 de octubre, que van a facilitar el uso efectivo de los medios electrónicos de la Administración, y el desarrollo necesario de las citadas leyes. La norma es acorde con el principio de proporcionalidad al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento jurídico, estableciéndose un marco normativo estable, integrado y claro. Asimismo, durante el procedimiento de elaboración de la norma, se han formalizado los trámites de consulta pública previa e información pública, que establece la Ley en cumplimiento del principio de transparencia, quedando además justificados en el preámbulo los objetivos que persigue este real decreto. Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación, en materia de cargas administrativas, respecto de las leyes que con esta norma se desarrollan.

Asimismo, el proyecto ha sido informado por la Agencia Española de Protección de Datos y se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y a informe de los diferentes ministerios.

El real decreto se dicta en ejercicio de la habilitación normativa contenida en la disposición final sexta de la Ley 39/2015, de 1 de octubre, y en la disposición final decimoquinta de la Ley 40/2015, de 1 de octubre, para llevar a cabo su desarrollo reglamentario en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público y garantizar, así, la efectiva aplicación e implantación de las previsiones que ambas leyes establecen, todo ello al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución. Los artículos 15,16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital y del Ministro de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 30 de marzo de 2021,

DISPONGO:

Artículo único. *Aprobación del Reglamento de actuación y funcionamiento del sector público por medios electrónicos.*

Se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Destrucción de documentos en soporte no electrónico.*

1. Transcurridos dos años desde la entrada en vigor de este real decreto, los documentos en soporte no electrónico que se encuentren en las oficinas de asistencia en materia de registros y de los que se haya obtenido una copia electrónica auténtica de conformidad con los requisitos que establece el Esquema Nacional de Interoperabilidad y su

normativa técnica complementaria, para su registro e incorporación al correspondiente expediente electrónico, podrán ser eliminados en las mismas condiciones que establece este real decreto.

Para ello será necesaria la comunicación previa a la autoridad calificadora correspondiente, que irá acompañada de un análisis de riesgos, con la especificación de las garantías de conservación de las copias electrónicas y del cumplimiento de las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establezca el Esquema Nacional de Seguridad, la normativa de transparencia, acceso a la información pública y buen gobierno, la legislación de archivos y patrimonio histórico y cultural y la normativa específica que sea de aplicación.

2. Asimismo, transcurridos dos años desde la entrada en vigor de este real decreto podrán destruirse las copias en papel de los documentos previstos en el artículo 49 del Reglamento que se encuentren en las oficinas de registro y de las que se haya obtenido en su momento la correspondiente copia electrónica.

Disposición transitoria segunda. *Portales de internet existentes y aplicaciones específicas en el ámbito estatal.*

1. La supresión de los portales de internet creados en el ámbito estatal antes de la entrada en vigor de este real decreto se regirá por las reglas aplicables en el momento de su creación.

2. En el plazo de seis meses desde la entrada en vigor de este real decreto, en el ámbito de cada ministerio se analizará la oportunidad del mantenimiento de sus portales de internet existentes y los de sus organismos públicos o entidades de derecho público vinculados o dependientes respectivos, así como de las páginas web promocionales («microsites»). Para ese análisis se aplicarán los mismos criterios previstos en el artículo 6 para la creación de nuevos portales y se decidirá acerca de su mantenimiento o su supresión.

En caso de que se decida la supresión, se valorará si es pertinente o no incorporar en el PAGe de la Administración General del Estado la información que se ha contenido en dichos portales hasta la supresión.

3. Realizado el proceso previsto en el apartado anterior, en el plazo máximo de un año desde la entrada en vigor de este real decreto se publicará en el PAGe de la Administración General del Estado una Resolución del Secretario General de Función Pública, en la que figurará el listado de portales de internet activos de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes de esta.

4. En el plazo máximo de un año desde la entrada en vigor de este real decreto, y a partir de la información facilitada por los ministerios, la Secretaría General de Administración Digital realizará el censo de aplicaciones específicas diseñadas para dispositivos móviles («app») para su utilización en los procedimientos de la Administración General del Estado.

5. En el ámbito de la Administración General del Estado, los portales de internet muy reconocidos e identificables por los usuarios, creados antes de la entrada en vigor de este real decreto se regirán por las reglas aplicables en el momento de su creación en cuanto a nomenclatura, sin necesidad de que modifiquen el nombre del dominio de segundo nivel.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto y, en concreto, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Disposición final primera. *Títulos competenciales.*

1. Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de procedimiento administrativo común y para dictar las bases del régimen jurídico de las Administraciones Públicas.

2. Los artículos 15, 16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento que aprueba este real decreto, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

3. No tiene carácter básico y será de aplicación únicamente en el ámbito estatal lo dispuesto en:

a) La disposición transitoria segunda y la disposición final tercera de este real decreto.

b) El segundo párrafo del apartado 3 del artículo 3, los artículos 6, 7.4, 8, 10.3, 10.4, 13.2, 17, 18.2, 19.3, 19.4, 21.4, 23.2, 24, 25.4, 28.3, 30.2, 31, 33, 36, 38.1, el segundo párrafo del apartado 4 del artículo 39, los artículos 40, 42.5, 48, 53.5, 55.2, 57, 60.3, 62.2 y las disposiciones adicionales primera, segunda, cuarta, quinta, sexta, el segundo apartado de la disposición adicional séptima del Reglamento que aprueba este real decreto.

[. . .]

Disposición final cuarta. *Habilitación normativa.*

Se faculta a la persona titular del Ministerio de Política Territorial y Función Pública y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital en el ámbito de sus competencias, para dictar las disposiciones y adoptar las medidas necesarias para el desarrollo y ejecución de este real decreto y del Reglamento que aprueba, así como para modificar el anexo del mismo.

Disposición final quinta. *Entrada en vigor.*

Este real decreto entrará en vigor el día 2 de abril de 2021.

REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. Este Reglamento tiene por objeto el desarrollo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referido a la actuación y el funcionamiento electrónico del sector público.

2. El ámbito subjetivo de aplicación es el establecido en el artículo 2 de la Ley 39/2015, de 1 de octubre, y el artículo 2 de la Ley 40/2015, de 1 de octubre.

Artículo 2. *Principios generales.*

El sector público deberá respetar los siguientes principios en sus actuaciones y relaciones electrónicas:

a) Los principios de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, el sector público utilizará estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado.

Las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán

disponibles de forma general y serán compatibles con los productos informáticos de uso general.

b) El principio de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

c) El principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias, de forma que se minimice el grado de conocimiento necesario para el uso del servicio.

d) El principio de interoperabilidad, entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

e) El principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos.

f) El principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Artículo 3. *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los sujetos a los que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar el procedimiento haya tenido constancia de la misma.

3. De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

A tal efecto, en el ámbito estatal la mencionada obligatoriedad de relacionarse por medios electrónicos con sus órganos, organismos y entidades de derecho público podrá ser establecida por real decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Asimismo, se publicará en el Punto de Acceso General electrónico (PAGe) de la Administración General del Estado y en la sede electrónica o sede asociada que corresponda.

Artículo 4. *Canales de asistencia para el acceso a los servicios electrónicos.*

Las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito competencial a través de alguno o algunos de los siguientes canales:

a) Presencial, a través de las oficinas de asistencia que se determinen.

b) Portales de internet y sedes electrónicas.
c) Redes sociales.
d) Telefónico.
e) Correo electrónico.
f) Cualquier otro canal que pueda establecerse de acuerdo con lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre.

TÍTULO I

Portales de internet, Punto de Acceso General electrónico y sedes electrónicas

Artículo 5. *Portales de internet de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 39 de la Ley 40/2015, de 1 de octubre, se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información y, en su caso, a la sede electrónica o sede electrónica asociada correspondiente.
2. Cada Administración podrá determinar los contenidos y canales mínimos de atención a las personas interesadas y de difusión y prestación de servicios que deban tener sus portales, así como criterios obligatorios de imagen institucional. En cualquier caso, deberán tenerse en cuenta los contenidos, formatos y funcionalidades que en la normativa de reutilización, accesibilidad y transparencia se establezcan como obligatorios para los sitios web.
3. Los portales de internet dispondrán de sistemas que permitan el establecimiento de medidas de seguridad de acuerdo con lo establecido en Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Artículo 6. *Creación y supresión de portales de internet en el ámbito estatal.*

1. En el ámbito estatal, la creación o supresión de portales se llevará a cabo por orden de la persona titular del ministerio correspondiente o por resolución de la persona titular del órgano superior, en el caso de la Administración General del Estado, y por resolución de la persona titular de la Presidencia o de la Dirección en el caso de sus organismos públicos y entidades de derecho público vinculados o dependientes.

La creación requerirá informe favorable de la Comisión Ministerial de Administración Digital respectiva y posterior comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital. Para obtener dicho informe favorable, la propuesta de creación del nuevo portal se deberá justificar en términos de eficiencia en la asignación y utilización de los recursos públicos e interés prioritario para la implantación de una política pública o la aplicación de la normativa de la Unión Europea o nacional y a tal efecto el órgano promotor de la creación del nuevo portal remitirá una memoria justificativa y económica.

La supresión de portales requerirá la previa comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital.

2. El acto o resolución de creación de un nuevo portal previsto en el apartado anterior contendrá, al menos, la identificación de su dirección electrónica, que deberá incluir el nombre de dominio de segundo nivel «.gob.es», su ámbito funcional y, en su caso, orgánico y la finalidad para la que se crea. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado.
3. En el ámbito estatal los portales de internet a los que se refiere este artículo deberán estar referenciados en el PAGe de la Administración General del Estado.

Artículo 7. *Punto de Acceso General electrónico.*

1. Las Administraciones Públicas contarán con un Punto de Acceso General electrónico (PAGe).

2. El PAGe de cada Administración Pública facilitará el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente.

3. El PAGe dispondrá de una sede electrónica, a través de la cual se podrá acceder a todas las sedes electrónicas y sedes asociadas de la Administración Pública correspondiente.

Además, esta sede podrá incluir un área personalizada a través de la cual cada interesado, mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos personales, podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente.

4. El PAGe de la Administración General del Estado y su sede electrónica serán gestionados por el Ministerio de Política Territorial y Función Pública en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

En dicha sede electrónica está alojada la Dirección Electrónica Habilitada única a la que se refiere el artículo 43 de la Ley 39/2015, de 1 de octubre.

El PAGe de la Administración General del Estado, a través de su sede, permitirá la comprobación de la autenticidad e integridad de los documentos facilitados por el sector público estatal a través del Código Seguro de Verificación o de cualquier otro sistema de firma o sello basado en certificado electrónico cualificado que se haya utilizado en su generación. También permitirá, en su caso, su recuperación.

5. El PAGe de la Administración General del Estado podrá interoperar con portales web oficiales de la Unión Europea.

Artículo 8. *Carpeta Ciudadana del sector público estatal.*

1. La Carpeta Ciudadana es el área personalizada de las personas interesadas a que se refiere el artículo 7.3 en su relación con el sector público estatal. Además del interesado podrán acceder a la Carpeta Ciudadana:

a) Sus representantes legales.

b) Quien ostente un poder general previsto en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre, otorgado por el interesado e inscrito en el Registro Electrónico de Apoderamientos.

2. La Carpeta Ciudadana será accesible a través de la sede electrónica del PAGe de la Administración General del Estado y podrá ofrecer, entre otras, las funcionalidades siguientes para el interesado o sus representantes:

a) Permitir el seguimiento del estado de tramitación de los procedimientos en que sea interesado, de acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/ 2015, de 1 de octubre.

b) Permitir el acceso a sus comunicaciones y notificaciones.

c) Conocer qué datos suyos obran en poder del sector público estatal, sin perjuicio de las limitaciones que establezca la normativa vigente.

d) Facilitar la obtención de certificaciones administrativas exigidas por la normativa correspondiente.

3. El interesado accederá a la Carpeta Ciudadana mediante los sistemas de identificación a los que se refiere el artículo 9.2 de la Ley 39/2015, de 1 de octubre.

4. El interesado deberá asegurar el buen uso de los sistemas de identificación y velar por que el acceso a su carpeta Ciudadana solo se haga por sí mismo o por tercero autorizado.

Artículo 9. *Sedes electrónicas de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, una sede electrónica es aquella dirección electrónica disponible para la ciudadanía por medio de redes de telecomunicaciones. Mediante dicha sede electrónica se realizarán todas las actuaciones y trámites referidos a procedimientos o a servicios que requieran la

identificación de la Administración Pública y, en su caso, la identificación o firma electrónica de las personas interesadas.

2. La titularidad de la sede electrónica corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ámbito de sus competencias.

Artículo 10. *Creación y supresión de las sedes electrónicas y sedes electrónicas asociadas.*

1. Se podrán crear una o varias sedes electrónicas asociadas a una sede electrónica atendiendo a razones técnicas y organizativas. La sede electrónica asociada tendrá consideración de sede electrónica a todos los efectos.

2. El acto o resolución de creación o supresión de una sede electrónica o sede electrónica asociada será publicado en el boletín oficial que corresponda en función de cuál sea la Administración Pública titular de la sede o sede asociada y también en el directorio del Punto de Acceso General Electrónico que corresponda. En el caso de las entidades locales, el boletín oficial será el de la provincia al que pertenezca la entidad.

El acto o resolución de creación determinará, al menos:

a) El ámbito de aplicación de la sede electrónica o sede electrónica asociada.

b) La identificación de la dirección electrónica de referencia de la sede electrónica o sede electrónica asociada que se cree, así como de las direcciones electrónicas de las sedes electrónicas que desde el momento de la creación ya sean asociadas de aquella. Las sedes electrónicas asociadas con posterioridad a la publicación del instrumento de creación se referenciarán en la mencionada dirección electrónica.

c) La identificación de su titular.

d) La identificación del órgano u órganos encargados de la gestión y de los servicios puestos a disposición en la misma.

3. En el ámbito estatal, tanto la creación o supresión de una sede electrónica asociada a la sede electrónica del PAGe de la Administración General del Estado como la creación o supresión de sedes electrónicas o sedes electrónicas asociadas de los organismos públicos y entidades de derecho público vinculados o dependientes se hará mediante orden de la persona titular del Departamento competente o por resolución de la persona titular de la Presidencia o de la Dirección del organismo o entidad de derecho público competente, con el informe previo favorable del Ministerio de Política Territorial y Función Pública y del Ministerio de Asuntos Económicos y Transformación Digital.

4. Para obtener los informes previos favorables a que se refiere el apartado anterior, la propuesta de creación de la nueva sede electrónica o, en su caso, sede electrónica asociada se tendrá que justificar, en términos de eficiencia en la asignación y utilización de recursos públicos. A tal efecto, el órgano promotor de la creación de la sede electrónica remitirá una memoria justificativa y económica en que se explicite el volumen de trámites que está previsto gestionar a través de la misma, los efectos presupuestarios y económicos de su establecimiento, su incidencia en la reducción del tiempo de resolución de los procedimientos y de cargas administrativas para las personas interesadas y cualquier otra razón de interés general que justifique su creación.

Artículo 11. *Contenido y servicios de las sedes electrónicas y sedes asociadas.*

1. Toda sede electrónica o sede electrónica asociada dispondrá del siguiente contenido mínimo a disposición de las personas interesadas:

a) La identificación de la sede electrónica o sede electrónica asociada, así como del órgano u organismo titular de la misma y los órganos competentes para la gestión de la información, servicios, procedimientos y trámites puestos a disposición en ella.

b) La identificación del acto o disposición de creación y el acceso al mismo, directamente o mediante enlace a su publicación en el Boletín Oficial correspondiente.

c) La información necesaria para la correcta utilización de la sede electrónica, incluyendo su mapa o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relativa a propiedad intelectual, protección de datos personales y accesibilidad.

d) La relación de sistemas de identificación y firma electrónica que sean admitidos o utilizados en la misma.

e) La normativa reguladora del Registro al que se acceda a través de la sede electrónica.

f) La fecha y hora oficial, así como el calendario de días inhábiles a efectos del cómputo de plazos aplicable a la Administración en que se integre el órgano, organismo público o entidad de derecho público vinculado o dependiente que sea titular de la sede electrónica o sede electrónica asociada.

g) Información acerca de cualquier incidencia técnica que acontezca e imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, así como de la ampliación del plazo no vencido que, en su caso, haya acordado el órgano competente debido a dicha circunstancia.

h) Relación actualizada de los servicios, procedimientos y trámites disponibles

i) Relación actualizada de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites descritos en la letra anterior. Cada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje.

2. Las sedes electrónicas y sedes electrónicas asociadas dispondrán, al menos, de los siguientes servicios a disposición de las personas interesadas:

a) Un acceso a los servicios y trámites disponibles en la sede electrónica o sede electrónica asociada, con indicación de los plazos máximos de duración de los procedimientos, excluyendo las posibles ampliaciones o suspensiones que en su caso, pudiera acordar el órgano competente.

b) Un enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

c) Los mecanismos de comunicación y procedimiento de reclamación establecidos al respecto de los requisitos de accesibilidad de los sitios web y aplicaciones móviles del sector público.

d) Un sistema de verificación de los certificados de la sede electrónica.

e) Un sistema de verificación de los sellos electrónicos de los órganos, organismos públicos o entidades de derecho público que abarque la sede electrónica o sede electrónica asociada.

f) Un servicio de comprobación de la autenticidad e integridad de los documentos emitidos por los órganos, organismos públicos o entidades de derecho público comprendidos en el ámbito de la sede electrónica, que hayan sido firmados por cualquiera de los sistemas de firma conformes a la Ley 40/2015, 1 de octubre, y para los cuales se haya generado un código seguro de verificación.

g) Un acceso a los modelos, y sistemas de presentación masiva, de uso voluntario, que permitan a las personas interesadas presentar simultáneamente varias solicitudes en la forma que establezca, en su caso, cada Administración, organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

h) El acceso a los modelos normalizados de presentación de solicitudes que establezca, en su caso, cada Administración u organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

i) Un servicio de consulta del directorio geográfico de oficinas de asistencia en materia de registros, que permita al interesado identificar la más próxima a su dirección de consulta.

3. De acuerdo con lo previsto en el artículo 66.1 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas deberán mantener y actualizar en la sede electrónica correspondiente un listado con los códigos de identificación vigentes de sus órganos, centros o unidades administrativas.

Artículo 12. *Responsabilidad sobre la sede electrónica o sede electrónica asociada.*

1. El titular de la sede electrónica y, en su caso, de la sede electrónica asociada, será responsable de la integridad, veracidad y actualización de la información y los servicios de su competencia a los que pueda accederse a través de la misma.

2. En caso de que la sede electrónica o sede electrónica asociada contenga un enlace o vínculo a otra sede o sede asociada, será el titular de esta última el responsable de la

integridad, veracidad y actualización de la información o procedimientos que figuren en la misma, sin perjuicio de la debida diligencia del titular de la primera respecto de la incorporación de los contenidos en la misma.

3. En caso de que una sede electrónica o sede electrónica asociada contenga procedimientos, servicios o ambos, cuya competencia corresponda a otro órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente, sea de la misma o de diferente Administración, el titular de la competencia será responsable de la integridad, veracidad y actualización de lo relativo a dichos procedimientos, servicios o ambos sin perjuicio de la debida diligencia del titular de la sede electrónica o sede electrónica asociada respecto de la incorporación de los contenidos en la misma.

TÍTULO II

Procedimiento administrativo por medios electrónicos

CAPÍTULO I

Disposiciones generales

Artículo 13. *Actuación administrativa automatizada.*

1. La tramitación electrónica de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada de acuerdo con lo previsto en el artículo 41 de la Ley 40/2015, de 1 de octubre.

2. En el ámbito estatal la determinación de una actuación administrativa como automatizada se autorizará por resolución del titular del órgano administrativo competente por razón de la materia o del órgano ejecutivo competente del organismo o entidad de derecho público, según corresponda, y se publicará en la sede electrónica o sede electrónica asociada. La resolución expresará los recursos que procedan contra la actuación, el órgano administrativo o judicial, en su caso, ante el que hubieran de presentarse y plazo para interponerlos, sin perjuicio de que las personas interesadas puedan ejercitar cualquier otro que estimen oportuno y establecerá medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de las personas interesadas.

3. En el ámbito de las Entidades Locales, en caso de actuación administrativa automatizada se estará a lo dispuesto en la disposición adicional octava del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.

Artículo 14. *Régimen de subsanación.*

1. Si existe la obligación del interesado de relacionarse a través de medios electrónicos y aquel no los hubiese utilizado, el órgano administrativo competente en el ámbito de actuación requerirá la correspondiente subsanación, advirtiendo al interesado, o en su caso su representante, que, de no ser atendido el requerimiento en el plazo de diez días, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de la Ley 39/2015, de 1 de octubre.

Este régimen de subsanación será asimismo aplicable a las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas que, de acuerdo con lo dispuesto en el artículo 3.2, hayan ejercitado su derecho a relacionarse electrónicamente con la Administración Pública de que se trate.

Cuando se trate de una solicitud de iniciación del interesado, la fecha de la subsanación se considerará a estos efectos como fecha de presentación de la solicitud de acuerdo con el artículo 68.4 de dicha ley.

2. De acuerdo con lo establecido en el artículo 39.1 de este Reglamento, en el caso de que las Administraciones Públicas hayan determinado los formatos y estándares a los que deberán ajustarse los documentos presentados por el interesado, si este incumple dicho requisito se le requerirá para que, en el plazo de diez días, subsane el defecto advertido en

los términos establecidos en los artículos 68.1, cuando se trate de una solicitud de iniciación, y 73.2, cuando se trate de otro acto, ambos de la Ley 39/2015, de 1 de octubre, con la indicación de que, si así no lo hiciera y previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de dicha ley, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, respectivamente.

3. En el caso de que el escrito o solicitud presentada adolezca de cualquier otro defecto subsanable, por la falta de cumplimiento de los requisitos exigidos en los artículos 66, 67 y 73 de la Ley 39/2015, de 1 de octubre, o por la falta de otros requisitos exigidos por la legislación específica aplicable, se requerirá su subsanación en el plazo de diez días, en los términos de los artículos 68.1 y 73.1 de la citada ley. Este plazo podrá ser ampliado hasta cinco días, a petición del interesado o a iniciativa del órgano, cuando la aportación de los documentos requeridos, en su caso, presente dificultades especiales, siempre que no se trate de procedimientos selectivos o de concurrencia competitiva.

CAPÍTULO II

De la identificación y autenticación de las Administraciones Públicas y las personas interesadas

Sección 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad

Artículo 15. *Sistemas de identificación, firma y verificación.*

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la normativa vigente sobre firma electrónica y resulten adecuados para garantizar la identificación de las personas interesadas y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para garantizar el origen e integridad de los documentos electrónicos:

a) Sistemas de identificación de las sedes electrónicas y sedes electrónicas asociadas.

b) Sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica.

c) Sistemas de firma electrónica para la actuación administrativa automatizada.

d) Firma electrónica del personal al servicio de las Administraciones Públicas.

e) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las Administraciones Públicas:

a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

b) Asimismo, se considerarán válidos a efectos de firma electrónica ante las Administraciones Públicas los sistemas previstos en las letras a), b) y c) del artículo 10.2 de la Ley 39/2015, de 1 de octubre.

c) De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

4. La Administración no será responsable de la utilización por terceras personas de los medios de identificación personal y firma electrónica del interesado, salvo que concurran los requisitos establecidos en el artículo 32 de la Ley 40/2015, de 1 de octubre, para la exigencia de responsabilidad patrimonial.

Artículo 16. *Plataformas de verificación de certificados electrónicos y de otros sistemas de identificación.*

1. La Administración General del Estado dispondrá de una plataforma para la verificación de la vigencia y del contenido de los certificados cualificados admitidos en el sector público. El sistema deberá permitir que tal verificación se pueda llevar a cabo de forma libre y gratuita, para el sector público.

La Secretaría General de Administración Digital será el órgano responsable de esta plataforma, que estará disponible para todo el sector público previa formalización del correspondiente instrumento de adhesión.

2. Esta plataforma dispondrá de una declaración de prácticas de validación en la que se detallarán las obligaciones que se comprometen a cumplir tanto la plataforma como las personas usuarias de la misma en relación con los servicios de verificación. Esta declaración estará disponible al público por vía electrónica y con carácter gratuito.

3. Los prestadores cualificados de servicios de confianza deberán facilitar a esta plataforma el acceso electrónico y gratuito para la verificación de la vigencia de los certificados electrónicos emitidos por aquellos en virtud de su cualificación de acuerdo con la legislación aplicable en materia de servicios electrónicos de confianza.

Artículo 17. *Política de firma electrónica y de certificados en el ámbito estatal.*

1. La política de firma electrónica y de certificados en el ámbito estatal, está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica.

2. Sin perjuicio de las obligaciones de los prestadores de servicios de confianza previstas en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y resto de normativa vigente, la política de firma electrónica y certificados deberá contener en todo caso:

a) La definición de su ámbito de aplicación.

b) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes.

c) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de confianza asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado y de sus organismos públicos y entidades vinculados o dependientes recogidas en este Reglamento.

3. La política de firma electrónica y certificados en el ámbito estatal será aprobada por Resolución de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial y se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del PAGe de la Administración General del Estado.

Sección 2.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia

Artículo 18. *Identificación de las sedes electrónicas y de las sedes electrónicas asociadas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas y sedes electrónicas asociadas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados cualificados de autenticación de sitio web o medio equivalente. Dichos certificados electrónicos se ajustarán a lo señalado en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, y la normativa vigente en materia de identidad y firma electrónica.

2. En el ámbito estatal las sedes electrónicas y sedes electrónicas asociadas se identificarán mediante certificados cualificados de autenticación de sitio web.

Con carácter adicional y para su identificación inmediata, los ciudadanos y ciudadanas dispondrán de la información general obligatoria que debe constar en las mismas de acuerdo con lo establecido en este Reglamento. Las direcciones electrónicas que tengan la condición de sede electrónica o sede electrónica asociada deberán hacerlo constar de forma visible e inequívoca. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio «.gob.es».

Artículo 19. *Identificación mediante sello electrónico basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.*

1. De acuerdo con lo previsto en el artículo 40 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

2. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos, publicándose en la sede electrónica o sede asociada o en el portal de internet correspondiente. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

3. En el ámbito estatal, la creación de sellos electrónicos se realizará mediante resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, que se publicará en la sede electrónica o sede electrónica asociada correspondiente. En dicha resolución deberá constar:

a) El órgano, organismo público o entidad de derecho público vinculado o dependiente titular del sello, que será el responsable de su utilización, con indicación de su Ministerio de adscripción, vinculación o dependencia.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y procedimientos en los que podrá ser utilizado.

4. Los certificados de sello electrónico en el ámbito estatal tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».

b) Nombre del suscriptor.

c) Número de identificación fiscal del suscriptor.

Artículo 20. *Sistemas de firma electrónica para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42 de la Ley 40/2015, de 1 de octubre, en la tramitación administrativa automatizada de los procedimientos, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes cuando estas tramiten procedimientos de forma automatizada en el ejercicio de potestades administrativas.

Artículo 21. *Sistemas de firma basados en código seguro de verificación para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42.b) de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas.

Dicho código vinculará al órgano, organismo público o entidad de derecho público y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento en la sede electrónica o sede electrónica asociada correspondiente mediante un procedimiento de verificación directo y gratuito para las personas interesadas.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El origen e integridad de los documentos mediante el acceso a la sede electrónica o sede electrónica asociada correspondiente.

b) El carácter único del código generado para cada documento.

c) Su vinculación con el documento generado y, en su caso, con el firmante. El código seguro de verificación y la dirección electrónica de acceso a la sede electrónica o sede electrónica asociada deberán integrarse preferentemente en todas las páginas del documento firmado con dicho código. Cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente.

d) La posibilidad de verificar el documento en la sede electrónica o sede electrónica asociada, como mínimo, por el tiempo que se establezca en la resolución que autorice la utilización de este procedimiento. Una vez que el documento deje de estar disponible en la sede electrónica o sede electrónica asociada, su disponibilidad por otros cauces se regirá por lo dispuesto en la estrategia de conservación implantada por cada Administración Pública a través de su política de gestión documental.

e) Un acceso restringido al documento a quien disponga del código seguro de verificación, sin perjuicio de las garantías adicionales que se puedan establecer.

3. En las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas, la interoperabilidad se garantizará mediante la superposición al código seguro de verificación de un sello electrónico de los previstos en el artículo 42 de la Ley 40/2015, de 1 de octubre, como mecanismo de verificación automática del origen e integridad de los documentos electrónicos en los términos que establezca la Norma Técnica de Interoperabilidad de Documento Electrónico.

4. En el ámbito estatal, la utilización de este sistema requerirá resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, previo informe del Centro Criptológico Nacional y de la Secretaría General de Administración Digital.

La orden o resolución de creación deberá incluir:

a) Actuaciones a las que es de aplicación el sistema.

b) Órganos responsables de la aplicación del sistema.

c) Disposiciones que resultan de aplicación a la actuación.

d) Sede electrónica o sede electrónica asociada a la que pueden acceder las personas interesadas para la verificación del contenido de la actuación o documento.

e) Plazo de disponibilidad para la verificación en la sede electrónica o sede electrónica asociada del código seguro de verificación aplicado a un documento. Este plazo será al menos de cinco años, salvo que en la normativa especial por razón de la materia se prevea un plazo superior. Transcurrido este tiempo, será necesario solicitarlo al órgano de la Administración Pública, organismo público o entidad de derecho público que emitió el documento. En este caso, cuando utilice medios electrónicos, la certificación de la

verificación se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público que tenga atribuida la actuación por aquel órgano.

Artículo 22. *Sistemas de firma electrónica del personal al servicio de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 43 de la Ley 40/2015, de 1 de octubre, sin perjuicio de lo previsto en los artículos 18, 19 y 20 de este Reglamento, la actuación de una Administración Pública, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público a través del que se ejerza la competencia.
2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal. Estos sistemas podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.
3. Los certificados electrónicos de empleado público serán cualificados y se ajustarán a lo señalado en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica.
4. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes de esta cuando tramiten procedimientos en el ejercicio de potestades administrativas.

Artículo 23. *Certificados electrónicos de empleado público con número de identificación profesional.*

1. Sin perjuicio de lo previsto en el artículo 22.3 de este Reglamento, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, los prestadores cualificados de servicios de confianza podrán consignar un número de identificación profesional en el certificado electrónico de empleado público, a petición de la Administración en la que presta servicios el empleado o empleada de que se trate, si dicho certificado se va a utilizar en actuaciones que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones para cuya realización esté legalmente justificado el anonimato. Estos certificados se denominarán «certificados electrónicos de empleado público con número de identificación profesional».
2. En el ámbito estatal corresponderá solicitar la consignación de un número de identificación profesional del empleado o empleada público a la persona titular de la Subsecretaría del ministerio o a la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público en el que preste servicios el empleado o empleada público.
3. La Administración solicitante del certificado conservará la documentación acreditativa de la identidad del titular.
4. Los certificados electrónicos de empleado público con número de identificación profesional serán cualificados y se ajustarán a lo previsto en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica y tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público, aunque limitados a las actuaciones que justificaron su emisión.
5. Las autoridades públicas competentes y los órganos judiciales, en el ejercicio de sus funciones y de acuerdo con la normativa vigente, podrán solicitar la revelación de la identidad del titular de un certificado de empleado público con número de identificación profesional mediante petición oficial dirigida a la Administración responsable de su custodia.

Artículo 24. *Sistemas de identificación y firma electrónica del personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. El personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, podrá identificarse con aquellos sistemas que, entre los previstos en la Ley 39/2015, de 1 de octubre, se establezcan en función del nivel de seguridad que corresponda al trámite de que se trate de acuerdo al Esquema Nacional de Seguridad.

2. Dicho personal podrá firmar mediante sistemas de firma electrónica basados en certificados electrónicos cualificados facilitados específicamente a sus empleados y empleadas. Estos sistemas podrán ser utilizados por estos en el desempeño efectivo de su puesto de trabajo, para los trámites y actuaciones que realicen por razón del mismo, o para relacionarse con las Administraciones públicas cuando estas lo admitan.

3. Se podrá disponer de sistemas de identificación de personal basados en repositorios de empleados públicos que permitan la relación de los empleados y empleadas públicos con servicios y aplicaciones necesarios para el ejercicio de sus funciones que en todo caso garanticen lo previsto en el Esquema Nacional de Seguridad.

4. Los registros de personal de la Administración General del Estado podrán recoger los datos para la identificación electrónica de los empleados y empleadas públicos, así como su cesión a sistemas de identificación de personal basados en repositorios de identidades de empleados públicos.

Artículo 25. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. De acuerdo con lo previsto en el artículo 44 de la Ley 40/2015, de 1 de octubre, los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, esta establecerá las condiciones y garantías por las que se regirá, que comprenderán, al menos, la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones Públicas, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En el ámbito estatal, las condiciones y garantías a que se refiere el apartado 2 serán establecidas por la Secretaría General de Administración Digital.

5. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan conforme a los requisitos establecidos en el Esquema Nacional de Seguridad

Sección 3.ª Identificación y firma de las personas interesadas

Artículo 26. *Sistemas de identificación de las personas interesadas en el procedimiento.*

1. De acuerdo con lo previsto en la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad.

2. En particular, de acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, serán admitidos los siguientes sistemas de identificación electrónica:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

Artículo 27. *Atributos mínimos de los certificados electrónicos cuando se utilizan para la identificación de las personas interesadas ante las Administraciones Públicas.*

1. Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca. La comprobación de la identidad y otras circunstancias de los solicitantes del certificado, se realizará de conformidad con lo previsto en el artículo 7 de la Ley 6/2020, de 11 de noviembre.

2. Los certificados electrónicos cualificados de representante de persona jurídica deberán contener, como mínimo, la denominación y el Número de Identificación Fiscal de la persona jurídica y el nombre y apellidos y número de Documento Nacional de Identidad, o Número de Identificación de Extranjero o Número de Identificación Fiscal de la persona que actúa como representante.

3. Los sistemas basados en certificados cualificados de sello electrónico admitidos por las Administraciones Públicas para la identificación electrónica de persona jurídica a que se refiere el artículo 9.2.b) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener, como mínimo, su denominación y su Número de Identificación Fiscal.

Artículo 28. *Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas.*

1. Los sistemas de clave concertada o cualquier otro sistema que las Administraciones Públicas consideren válidos, admitidos para la identificación electrónica de persona física de conformidad con el artículo 9.2.c) de la Ley 39/2015, de 1 de octubre, deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad y contener, como mínimo, el nombre y apellidos y el número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Fiscal y, para los casos en que así se establezca en la definición del sistema, el número de pasaporte.

2. Los sistemas de identificación a que se refiere el apartado anterior deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

3. En el ámbito estatal, la creación de los nuevos sistemas de identificación será aprobada por orden de la persona titular del Ministerio o, en su caso, resolución de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente por razón del ámbito material en que se vaya a utilizar, previa autorización de la Secretaría General de Administración Digital a que se refiere el apartado anterior.

Cuando el nuevo sistema se refiera a la totalidad de la Administración General del Estado se requerirá Acuerdo del Consejo de Ministros a propuesta de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En este caso, este sistema deberá estar accesible a través de la Plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Artículo 29. *Sistemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso.*

1. De acuerdo con lo previsto en el artículo 10.2 de la Ley 39/2015, de 1 de octubre, en el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuente con un registro previo como usuario que permita garantizar su identidad.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

2. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación del interesado y, en su caso, del representante o la representante, que sean necesarios de acuerdo con la legislación que le sea aplicable.

3. Los sistemas de firma electrónica que usen las personas interesadas permitirán que las Administraciones Públicas puedan verificar los datos consignados de la firma, de manera que se pueda vincular su identidad con el acto de firma.

4. Los sistemas de firma electrónica previstos en la letra c) del apartado 1 deberán contar con la previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. Asimismo, deberán cumplir con lo previsto en el Real Decreto 3/2010, de 8 de enero.

5. De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de las personas interesadas.

Artículo 30. *Identificación o firma electrónica de las personas interesadas mediante personal funcionario público habilitado.*

1. De acuerdo con lo previsto en el segundo párrafo del artículo 12.2 de la Ley 39/2015 de 1 de octubre, si algún interesado no incluido en los apartados 2 y 3 del artículo 14 de la ley no dispusiera de los medios electrónicos necesarios para su identificación o firma electrónica en el procedimiento administrativo, estas podrán ser válidamente realizadas por personal funcionario público habilitado mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado se identifique ante el funcionario o funcionaria y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia por escrito para los casos de discrepancia o litigio.

El funcionario habilitado entregará al interesado toda la documentación acreditativa del trámite realizado, así como una copia del documento de consentimiento expreso cumplimentado y firmado, cuyo formulario estará disponible en el Punto de Acceso General Electrónico de la respectiva Administración

2. En el ámbito estatal la identificación y firma electrónica del interesado conforme al procedimiento descrito en el apartado anterior se realizará necesariamente por un funcionario público inscrito a tal efecto en el Registro de Funcionarios Habilitados de la Administración General del Estado.

La identificación o firma electrónica en el procedimiento por personal funcionario público habilitado sólo será válida para los trámites y actuaciones que haya determinado con carácter previo cada ministerio, organismo público o entidad de derecho público vinculado o dependiente y en los términos que se especifiquen mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En el PAGe de la Administración General del Estado y en las sedes electrónicas asociadas de cada ministerio o en la sede electrónica o sede asociada del organismo público o entidad de derecho público en su ámbito de competencia, se mantendrá una relación pública, permanentemente actualizada, de dichos trámites y actuaciones.

Artículo 31. *Registro de Funcionarios Habilitados de la Administración General del Estado.*

1. Se crea el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, en el que constarán inscritos:

a) El personal funcionario habilitado para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen por el ministerio, organismo o entidad competente para su tramitación.

b) El personal funcionario habilitado para la expedición de copias auténticas. Esta habilitación será conferida por los órganos a los que corresponda la emisión de los documentos originales, su custodia, el archivo de documentos o que en sus normas de competencia así se haya previsto.

c) El personal funcionario habilitado que presta servicio en las oficinas de asistencia en materia de registros de la Administración General del Estado, que estará habilitados para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen y para la expedición de copias auténticas electrónicas de cualquier documento que estas presenten para que se remita desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. El Registro de Funcionarios Habilitados será gestionado por la Secretaría de Estado de Política Territorial y Función Pública del Ministerio de Política Territorial y Función Pública, en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Este Registro será interoperable con los sistemas equivalentes que ya existan en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

3. Este Registro deberá ser plenamente interoperable con los registros u otros sistemas equivalentes que se creen por las comunidades autónomas y las entidades locales a los efectos de comprobar la validez de las citadas habilitaciones.

4. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regulará el funcionamiento del Registro de Funcionarios Habilitados

Sección 4.ª Acreditación de la representación de las personas interesadas

Artículo 32. *Acreditación en la actuación por medio de representante.*

1. De acuerdo con lo previsto en el artículo 5 de la Ley 39/2015, de 1 de octubre, las personas interesadas con capacidad de obrar podrán actuar ante las Administraciones Públicas por medio de representante, bien sea una persona física con capacidad de obrar bien sea una persona jurídica cuando así esté previsto en sus Estatutos.

2. Los representantes de las personas interesadas obligadas a relacionarse electrónicamente con las Administraciones Públicas están obligados a relacionarse electrónicamente en el ejercicio de dicha representación, de acuerdo con el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

3. La representación puede acreditarse mediante cualquier medio válido en Derecho que deje constancia fidedigna de su existencia, entre otros:

a) Mediante apoderamiento apud acta efectuado por comparecencia personal en las oficinas de asistencia en materia de registros o comparecencia electrónica en la correspondiente sede electrónica o sede electrónica asociada.

b) Mediante acreditación de su inscripción en el registro electrónico de apoderamientos de la Administración Pública competente o en sus registros particulares de apoderamientos.

c) Mediante un certificado electrónico cualificado de representante.

d) Mediante documento público cuya matriz conste en un archivo notarial o de una inscripción practicada en un registro mercantil.

4. En el caso de actuaciones en nombre de persona jurídica, la capacidad de representación podrá acreditarse también mediante certificado electrónico cualificado de representante, entendiéndose en tal caso que el poder de representación abarca cualquier actuación ante cualquier Administración Pública.

5. Asimismo, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones por medios electrónicos en representación de las personas interesadas. En la sede electrónica o sede electrónica asociada de cada una de las Administraciones Públicas se publicarán los trámites electrónicos que podrán realizarse con esta representación.

Artículo 33. *Registro Electrónico de Apoderamientos de la Administración General del Estado.*

1. A los efectos previstos en el artículo anterior y de acuerdo con el artículo 6 de la Ley 39/2015, de 1 de octubre, en el Registro Electrónico de Apoderamientos de la Administración General del Estado se inscribirán los apoderamientos de carácter general previstos en el artículo 6.4.a) de dicha ley otorgados «apud acta» a favor de representante, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo para actuar en su nombre ante las Administraciones Públicas.

Asimismo, podrán inscribirse los poderes previstos en el artículo 6.4.b) de la ley para actuar ante la Administración General del Estado o ante un organismo público o entidad de Derecho Público vinculado o dependiente de la misma que no cuente con un registro electrónico de apoderamientos particular. Por último, podrán inscribirse los poderes previstos en el artículo 6.4.c) de la ley otorgados para realizar determinados trámites y actuaciones especificados en el poder ante los órganos de la Administración General del Estado o ante un organismo público o entidad de derecho público vinculado o dependiente de dicha Administración que no cuente con el citado registro particular.

Constará en el Registro el bastanteo del poder realizado por los servicios jurídicos correspondientes, sin perjuicio de la apreciación concreta de su suficiencia en la actuación, trámite o procedimiento en que se emplee.

2. El Registro Electrónico de Apoderamientos de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública con la colaboración del Ministerio de Asuntos Económicos y Transformación Digital, y será accesible desde la sede electrónica del PAGe de la Administración General del Estado así como desde las sedes y sedes electrónicas asociadas de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes.

3. Sin perjuicio de este registro general de apoderamientos, cada organismo público o entidad de derecho público vinculado o dependiente de la Administración General del Estado podrá disponer de un registro particular de apoderamientos en el que se inscriban los poderes otorgados por quien ostente la condición de interesado para realizar los trámites específicos de su competencia y cuya gestión corresponderá al propio organismo o entidad.

En estos registros particulares no podrán inscribirse los poderes previstos en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

4. El Registro Electrónico de Apoderamientos y los registros particulares deberán ser interoperables y no tienen carácter público, por lo que el interesado sólo podrá acceder a la información de los apoderamientos de los que sea poderdante o apoderado.

5. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y

Transformación Digital se regularán los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos de la Administración General del Estado.

Artículo 34. *Acreditación de la representación mediante certificado electrónico cualificado de representante.*

1. La representación podrá acreditarse ante la Administración con un certificado electrónico cualificado de representante de persona jurídica que sea acorde a lo previsto en el artículo 28 y el Anexo I del al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS) y a la Política marco de Firma Electrónica y de certificados a que hace referencia el Esquema Nacional de Interoperabilidad y, además, haya sido expedido a quien tenga un poder general para llevar a cabo cualquier actuación administrativa y ante cualquier Administración.

2. La aceptación de certificados electrónicos cualificados de representante de persona jurídica de alcance no general estará sujeta al Reglamento eIDAS, a la Política Marco de Firma Electrónica y de Certificados a que hace referencia el Esquema Nacional de Interoperabilidad y además, a los requisitos que disponga cada Administración.

Artículo 35. *Acreditación y verificación de las representaciones que resulten de un documento público notarial o certificación de un Registro Mercantil.*

1. Cuando la representación alegada resulte de un documento público notarial, o de una certificación expedida por un registro mercantil, el interesado deberá aportar la certificación registral electrónica correspondiente o al menos expresar el código seguro u otro sistema de acceso y verificación del documento electrónico.

2. Las Administraciones Públicas efectuarán la verificación de la autenticidad e integridad del traslado a papel y el acceso a los metadatos necesarios para la tramitación automatizada de la certificación registral electrónica, mediante el acceso electrónico y gratuito a la dirección electrónica que el Consejo General del Notariado o el Colegio de Registradores, respectivamente, habrán de tener habilitada a tales efectos.

3. Asimismo, las Administraciones Públicas, cuando necesiten comprobar la vigencia, revocación o cese de representaciones inscritas en el Registro Mercantil, consultarán electrónicamente y de modo gratuito el Registro Mercantil.

Artículo 36. *Autorización de representantes de terceros por la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. La Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de las personas interesadas.

2. La habilitación requerirá la firma previa de un convenio entre el Ministerio, organismo público o entidad de derecho público vinculado o dependiente competente y la organización o corporación de que se trate, de acuerdo de lo previsto en el capítulo VI del título Preliminar de la Ley 40/2015, de 1 de octubre. El convenio deberá especificar, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables tanto a la entidad firmante del convenio, como a las personas físicas o jurídicas habilitadas y determinará la presunción de validez de la representación.

A estos efectos, podrá acordarse un modelo normalizado de convenio que permita dar soporte a esta habilitación en los términos y condiciones que las partes acuerden, conforme a lo dispuesto en la Ley 40/2015, de 1 de octubre, y que incluya como anexo el modelo individualizado de adhesión al convenio que, previendo expresamente la aceptación de su contenido íntegro, deben suscribir las personas físicas o jurídicas miembros de las organizaciones o corporaciones firmantes que se adhieran al mismo.

3. De acuerdo con lo previsto en el artículo 32.5, en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, los trámites electrónicos que podrán realizarse con esta representación se publicarán en la sede electrónica del PAGe de la Administración General del Estado y en las respectivas sedes electrónicas o sedes electrónicas asociadas.

CAPÍTULO III

Registros, comunicaciones y notificaciones electrónicas

Sección 1.ª Registros electrónicos

Artículo 37. *Registro electrónico.*

1. Las Administraciones Públicas dispondrán de registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones, que deberán ser plenamente interoperables de manera que se garantice su compatibilidad informática e interconexión en los términos previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre y en el artículo 60 de este Reglamento.

2. Cada Administración dispondrá de un Registro Electrónico General en el que hará el asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente. Los organismos públicos y entidades de derecho público vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración a la que estén vinculados o de la que dependan.

3. Los registros electrónicos admitirán:

a) Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

b) Cualquier solicitud, escrito o comunicación distinta de los mencionados en el párrafo anterior dirigido a cualquier Administración Pública.

4. De acuerdo con el artículo 16.8 de la Ley 39/2015, de 1 de octubre, no se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación. En estos supuestos, el órgano administrativo competente para la tramitación del procedimiento comunicará esta circunstancia al interesado e informará de los requisitos exigidos por la legislación específica aplicable

Artículo 38. *Registro Electrónico General de la Administración General del Estado.*

1. El Registro Electrónico General de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital y se configura como el conjunto agregado de:

a) Los asientos practicados a través de las aplicaciones de que dispongan las unidades que realicen anotaciones en registro.

b) Las anotaciones que se realicen en cualquier aplicación que proporcione soporte a procedimientos específicos.

c) Las anotaciones que se practiquen por medio del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones que no dispongan de modelos normalizados de presentación, independientemente de las Administraciones Públicas u organismos públicos o entidades de derecho público vinculados o dependientes a las que vayan dirigidos. Dicho servicio electrónico será accesible desde la sede electrónica del PAGe de la Administración General del Estado.

2. Las anotaciones en el Registro General de la Administración General del Estado tendrán plena eficacia y validez para todas las Administraciones Públicas.

Artículo 39. *Presentación y tratamiento de documentos en registro.*

1. Las Administraciones Públicas podrán determinar los formatos y estándares a los que deberán ajustarse los documentos presentados por las personas interesadas en el registro siempre que cumplan con lo previsto en el Esquema Nacional de Interoperabilidad y normativa correspondiente.

2. En el caso de que se detecte código malicioso susceptible de afectar a la integridad o seguridad del sistema en documentos que ya hayan sido registrados, se requerirá su subsanación al interesado que los haya aportado de acuerdo con lo previsto en el artículo 14.3 de este Reglamento.

3. Los documentos en soporte no electrónico se presentarán a través de las oficinas de asistencia en materia de registros. Cuando se presenten documentos originales o copias auténticas en soporte no electrónico, desde el momento en que sean digitalizados conforme a lo dispuesto en las correspondientes normas técnicas de interoperabilidad, tendrán la consideración de copia electrónica auténtica de documento en soporte papel con la misma validez para su tramitación que los documentos aportados en soporte papel, conforme a las previsiones del artículo 27 de la Ley 39/2015, de 1 de octubre.

4. Cuando el tamaño de los documentos registrados exceda la capacidad que se determine para el Sistema de Interconexión de Registros (SIR), su remisión a la Administración y órgano al que van dirigidos podrá sustituirse por la puesta a disposición de los documentos, previamente depositados en un repositorio de intercambio de ficheros.

En ámbito de la Administración General del Estado dicho repositorio de intercambio de ficheros será de titularidad pública y tanto los documentos depositados como los datos que estos contengan no podrán ser utilizados para fines distintos a los previstos en la normativa que regule el procedimiento para el que han sido objeto de registro.

5. Los documentos presentados en las oficinas de asistencia en materia de registro serán devueltos a las personas interesadas inmediatamente tras su digitalización o, en caso contrario, se les aplicará lo previsto en el artículo 53 de este Reglamento.

6. El archivo de los documentos intercambiados por registro corresponderá al órgano competente para la tramitación del procedimiento, de acuerdo al plazo que determine su normativa.

Artículo 40. *Oficinas de asistencia en materia de registros en el ámbito de la Administración General del Estado.*

1. Las Oficinas de asistencia en materia de registros tienen naturaleza de órgano administrativo de acuerdo con lo dispuesto en el artículo 5 de la Ley 40/2015, de 1 de octubre.

La creación de nuevas Oficinas, así como la modificación o supresión de las existentes se realizará conforme a lo previsto en el artículo 59.2 de la Ley 40/2015, de 1 de octubre.

2. La Administración General del Estado contará con un directorio geográfico de las Oficinas de asistencia en materia de registros que será gestionado por el Ministerio de Política Territorial y Función Pública. A tal efecto, el órgano del que dependa la correspondiente Oficina de asistencia deberá comunicar de forma inmediata al citado Ministerio la aprobación de la norma por la que se cree, modifique o suprima dicha oficina, de acuerdo con lo establecido en el Esquema Nacional de Interoperabilidad, garantizando su actualización permanente.

3. Las Oficinas de asistencia en materia de registros desarrollarán las siguientes funciones:

a) La digitalización de las solicitudes, escritos y comunicaciones en papel que se presenten o sean recibidos en la Oficina y se dirijan a cualquier órgano, organismo público o entidad de derecho público de cualquier Administración Pública, así como su anotación en el Registro Electrónico General o Registro electrónico de cada organismo o entidad según corresponda.

b) La anotación, en su caso, de los asientos de salida que se realicen de acuerdo con lo dispuesto en el artículo 16 de la Ley 39/2015, de 1 de octubre.

c) La emisión del correspondiente recibo que acredite la fecha y hora de presentación de solicitudes, comunicaciones y documentos que presenten las personas interesadas.

d) La expedición de copias electrónicas auténticas tras la digitalización de cualquier documento original o copia auténtica que presenten las personas interesadas y que se vaya a incorporar a un expediente administrativo a través de dicha oficina en el registro electrónico correspondiente.

e) La información en materia de identificación y firma electrónica, para la presentación de solicitudes, escritos y comunicaciones a través de medios electrónicos en los trámites y procedimientos para los que se haya conferido habilitación.

f) La identificación o firma electrónica del interesado, cuando se trate de una persona no obligada a la relación electrónica con la Administración, en los procedimientos administrativos para los que se haya previsto habilitación.

g) La práctica de notificaciones, en el ámbito de actuación de esa Oficina, cuando el interesado o su representante comparezcan de forma espontánea en la Oficina y solicite la comunicación o notificación personal en ese momento.

h) La comunicación a las personas interesadas del código de identificación del órgano, organismo público o entidad a la que se dirige la solicitud, escrito o comunicación.

i) La iniciación de la tramitación del apoderamiento presencial apud acta en los términos previstos en el artículo 6 de la Ley 39/2015, de 1 de octubre.

j) Cualesquiera otras funciones que se les atribuyan legal o reglamentariamente.

Sección 2.ª Comunicaciones y notificaciones electrónicas

Artículo 41. *Comunicaciones administrativas a las personas interesadas por medios electrónicos.*

Cuando de acuerdo con lo previsto en el artículo 14 de la Ley 39/2015, de 1 de octubre, la relación de las personas interesadas con las Administraciones Públicas deba realizarse por medios electrónicos, serán objeto de comunicación al interesado por medios electrónicos, al menos:

a) La fecha y, en su caso, hora efectiva de inicio del cómputo de plazos que haya de cumplir la Administración tras la presentación del documento o documentos en el registro electrónico, de acuerdo con lo previsto en el artículo 31.2.c) de la Ley 39/2015, de 1 de octubre.

b) La fecha en que la solicitud ha sido recibida en el órgano competente, el plazo máximo para resolver el procedimiento y para la práctica de la notificación de los actos que le pongan término, así como de los efectos del silencio administrativo, de acuerdo con lo previsto en el artículo 21.4 de la Ley 39/2015, de 1 de octubre.

c) La solicitud de pronunciamiento previo y preceptivo a un órgano de la Unión Europea y la notificación del pronunciamiento de ese órgano de la Unión Europea a la Administración instructora de acuerdo con lo previsto en el artículo 22.1.b) de la Ley 39/2015, de 1 de octubre.

d) La existencia, desde que se tenga constancia de la misma, de un procedimiento no finalizado en el ámbito de la Unión Europea que condicione directamente el contenido de la resolución, así como la finalización de dicho procedimiento de acuerdo con lo previsto en el artículo 22.1.c) de la Ley 39/2015, de 1 de octubre.

e) La solicitud de un informe preceptivo a un órgano de la misma o distinta Administración y la recepción, en su caso, de dicho informe, de acuerdo con lo previsto en el artículo 22.1.d) de la Ley 39/2015, de 1 de octubre.

f) La solicitud de previo pronunciamiento de un órgano jurisdiccional, cuando este sea indispensable para la resolución del procedimiento, así como el contenido del pronunciamiento cuando la Administración actuante tenga la constancia del mismo de acuerdo con lo previsto en el artículo 22.1.g) de la Ley 39/2015, de 1 de octubre.

g) La realización del requerimiento de anulación o revisión de actos entre administraciones previsto en el artículo 22.2.a) de la Ley 39/2015, de 1 de octubre, así como su cumplimiento o, en su caso, la resolución del correspondiente recurso contencioso-administrativo.

Artículo 42. *Práctica de las notificaciones a través de medios electrónicos.*

1. De acuerdo con lo previsto en el artículo 43.1 de la Ley 39/2015, de 1 de octubre, las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica o sede electrónica asociada de la Administración, organismo público o entidad de derecho público vinculado o dependiente actuante, a través de la Dirección Electrónica Habilitada única o mediante ambos sistemas, según disponga cada Administración, organismo público o entidad de derecho público vinculado o dependiente, debiendo quedar constancia de la fecha y hora del acceso al contenido de la misma, o del rechazo de la notificación.

En caso de que la Administración, organismo o entidad actuante lleve a cabo la puesta a disposición de las notificaciones por ambos sistemas, para el cómputo de plazos y el resto de efectos jurídicos se tomará la fecha y hora de acceso al contenido o el rechazo de la notificación por el interesado o su representante en el sistema en el que haya ocurrido en primer lugar. A tal efecto se habrá de disponer de los medios electrónicos necesarios para sincronizar de forma automatizada en uno y otro sistema la información sobre el estado de la notificación con objeto de garantizar la eficacia y seguridad jurídica en la tramitación del procedimiento.

2. Con independencia de que un interesado no esté obligado a relacionarse electrónicamente con las Administraciones Públicas o de que no haya comunicado que se le practiquen notificaciones por medios electrónicos, su comparecencia voluntaria o la de su representante en la sede electrónica o sede asociada de una Administración, organismo público o entidad de derecho público vinculado o dependiente o a través de la Dirección Electrónica Habilitada única, y el posterior acceso al contenido de la notificación o el rechazo expreso de esta tendrá plenos efectos jurídicos.

3. La notificación por comparecencia en la sede electrónica o sede electrónica asociada y a través de la Dirección Electrónica Habilitada única conlleva la puesta a disposición del interesado de un acuse de recibo que permita justificar bien el acceso al contenido de la notificación, bien el rechazo del interesado a recibirla.

El acuse contendrá, como mínimo, la identificación del acto notificado y la persona destinataria, la fecha y hora en la que se produjo la puesta a disposición y la fecha y hora del acceso a su contenido o del rechazo.

4. En los supuestos de sucesión de personas físicas o jurídicas, inter vivos o mortis causa, la persona o entidad que sucede al interesado comunicará la sucesión al órgano competente de la tramitación del procedimiento de cuya existencia tenga conocimiento. Dicha comunicación deberá efectuarse tras la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física.

El órgano responsable de la tramitación procederá, en su caso, en procedimientos no finalizados, a autorizar a la persona o entidad sucesora el acceso a las notificaciones electrónicas ya practicadas desde la fecha del hecho causante de la sucesión y a practicar a dicha persona o entidad sucesora las notificaciones electrónicas que se produzcan en lo sucesivo. En el caso en el que la persona física sucesora no estuviera obligada a relacionarse electrónicamente con la Administración y no opte por este cauce de relación, las notificaciones que se produzcan en lo sucesivo deberán practicarse en papel, sin perjuicio de la garantía de acceso al expediente completo.

La persona o entidad que suceda al interesado en un procedimiento del que conozca su existencia debe comunicar, conforme a lo expuesto en los párrafos anteriores, la sucesión a la Administración Pública a la que corresponda la tramitación de aquel, en el plazo de 15 días hábiles, desde el día siguiente al de la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física. Si la persona o entidad sucesora efectúa la comunicación después de dicho plazo, los defectos en la práctica de notificaciones que se deriven de este incumplimiento, que hubieran acaecido con anterioridad a dicha comunicación, le serán imputables al interesado; dándose por cumplida por la Administración, a todos los efectos, la obligación de puesta a disposición de la notificación electrónica en la sede electrónica o sede electrónica asociada, a través de la Dirección Electrónica Habilitada única o ambas, según proceda, a la persona jurídica o persona física cuya sucesión el interesado no ha hecho valer.

5. Toda notificación cuyo emisor pertenezca al ámbito estatal a que se refiere el artículo 1.2 de este Reglamento se pondrá a disposición del interesado a través de la Dirección Electrónica Habilitada única, incluyendo el supuesto previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre. Asimismo, los emisores de ámbito estatal podrán notificar en su sede electrónica o sede electrónica asociada de forma complementaria a la puesta a disposición en la Dirección Electrónica Habilitada única.

Artículo 43. *Aviso de puesta a disposición de la notificación.*

1. De acuerdo con lo previsto en el artículo 41.6 de la Ley 39/2015, de 1 de octubre, con independencia de que la notificación se realice en papel o por medios electrónicos, las Administraciones Públicas, organismos públicos o entidades de derecho público vinculados o dependientes enviarán al interesado o, en su caso, a su representante, aviso informándole de la puesta a disposición de la notificación bien en la Dirección Electrónica Habilitada única, bien en la sede electrónica o sede electrónica asociada de la Administración, u Organismo o Entidad o, en su caso, en ambas.

La falta de práctica de este aviso, de carácter meramente informativo, no impedirá que la notificación sea considerada plenamente válida.

El aviso se remitirá al dispositivo electrónico o la dirección de correo electrónico que el interesado haya comunicado voluntariamente al efecto, o a ambos, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre.

El interesado se hace responsable, por la comunicación a la Administración, organismo público o entidad de derecho público vinculado o dependiente, de que dispone de acceso al dispositivo o dirección de correo electrónico designados. En caso de que dejen de estar operativos o pierda la posibilidad de acceso, el interesado está obligado a comunicar a la Administración que no se realice el aviso en tales medios. El incumplimiento de esta obligación por parte del interesado no conllevará responsabilidad alguna para la Administración por los avisos efectuados a dichos medios no operativos.

El aviso regulado en este apartado sólo se practicará en caso de que el interesado o su representante hayan comunicado a la Administración un dispositivo electrónico o dirección de correo electrónico al efecto.

2. Cuando el interesado sea un sujeto obligado a relacionarse por medios electrónicos y la Administración emisora de la notificación no disponga de datos de contacto electrónicos para practicar el aviso de su puesta a disposición, en los procedimientos iniciados de oficio la primera notificación que efectúe la Administración, organismo o entidad se realizará en papel en la forma determinada por el artículo 42.2 de la Ley 39/2015, de 1 de octubre, advirtiendo al interesado en esa primera notificación que las sucesivas se practicarán en forma electrónica por comparecencia en la sede electrónica o sede electrónica asociada que corresponda o, en su caso, a través de la Dirección Electrónica Habilitada única según haya dispuesto para sus notificaciones la Administración, organismo o entidad respectivo, y dándole a conocer que, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre, puede identificar un dispositivo electrónico, una dirección de correo electrónico o ambos para el aviso de la puesta a disposición de las notificaciones electrónicas posteriores.

3. Las Administraciones podrán crear bases de datos de contacto electrónico para la práctica de los avisos de puesta a disposición de notificaciones en su respectivo ámbito.

Artículo 44. *Notificación a través de la Dirección Electrónica Habilitada única.*

1. La Dirección Electrónica Habilitada única es el sistema de información para la notificación electrónica cuya gestión corresponde al Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública.

2. De acuerdo con lo previsto en el artículo 7.4, la Dirección Electrónica Habilitada única se aloja en la sede electrónica del PAGe de la Administración General del Estado.

3. La adhesión a la Dirección Electrónica Habilitada única se realizará en los términos previstos en el artículo 65.

Todas las Administraciones Públicas y sus organismos públicos y entidades de derecho público vinculados o dependientes colaborarán para establecer sistemas interoperables que

permitan que las personas físicas y jurídicas puedan acceder a todas sus notificaciones a través de la Dirección Electrónica Habilitada única, tal como establece el artículo 43 de la Ley 39/2015, de 1 de octubre.

Esta previsión será aplicable con independencia de cuál sea la Administración que practica la notificación y si las notificaciones se han practicado en papel o por medios electrónicos.

4. Cuando una incidencia técnica imposibilite el funcionamiento ordinario de la Dirección Electrónica Habilitada única, una vez comunicada dicha incidencia a los órganos, organismos o entidades emisores que la utilicen como medio de notificación, estos podrán determinar una ampliación del plazo no vencido para comparecer y acceder a las notificaciones emitidas. En caso de que también pongan a disposición las notificaciones en su sede electrónica o sede electrónica asociada, deberán publicar también en esta tanto la incidencia técnica acontecida en la Dirección Electrónica Habilitada única como la ampliación concreta, en su caso, del plazo no vencido.

5. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la Dirección Electrónica Habilitada única, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, dicho acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma, dará por efectuado el trámite de notificación y se continuará el procedimiento.

6. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la Dirección Electrónica Habilitada única deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la Dirección Electrónica Habilitada única se sincronizará automáticamente con la sede electrónica o sede electrónica asociada en la que, en su caso, la notificación también se hubiera puesto a disposición del interesado.

Artículo 45. *Notificación electrónica en sede electrónica o sede electrónica asociada.*

1. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la sede electrónica o sede electrónica asociada del emisor de la misma, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, la comparecencia y acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma dará por efectuado el trámite de notificación y se continuará el procedimiento.

2. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la sede electrónica o sede electrónica asociada deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la sede electrónica o sede electrónica asociada se sincronizará automáticamente con la Dirección Electrónica Habilitada única si la notificación también se hubiera puesto a disposición del interesado en aquella.

3. De conformidad con el artículo 43.3 de la Ley 39/2015, de 1 de octubre, se entenderá cumplida la obligación de notificar en plazo por parte de la Administración, a que se refiere el artículo 40.4 de dicha ley, con la puesta a disposición de la notificación en la sede o en la dirección electrónica habilitada única.

TÍTULO III

Expediente administrativo electrónico

CAPÍTULO I

Documento administrativo electrónico y copias

Artículo 46. *Documento administrativo electrónico.*

1. Se entiende por documento administrativo electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado admitido en el Esquema Nacional de Interoperabilidad y normativa correspondiente, y que haya sido generada, recibida o incorporada por las Administraciones Públicas en el ejercicio de sus funciones sujetas a Derecho administrativo.

2. Cuando en el marco de un procedimiento administrativo tramitado por medios electrónicos el órgano actuante esté obligado a facilitar al interesado un ejemplar de un documento administrativo electrónico, dicho documento se podrá sustituir por la entrega de los datos necesarios para su acceso por medios electrónicos adecuados.

Artículo 47. *Requisitos de validez y eficacia de las copias auténticas de documentos.*

1. De acuerdo con lo previsto en el artículo 27.2 de la Ley 39/2015, de 1 de octubre, tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

2. Las copias auténticas se expedirán siempre a partir de un original o de otra copia auténtica y tendrán la misma validez y eficacia que los documentos originales.

Artículo 48. *Órganos competentes para la emisión de copias auténticas de documentos en el ámbito estatal.*

1. En el ámbito estatal, serán competentes para la expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original los siguientes órganos:

a) Los órganos a los que corresponda la emisión de los documentos originales.

b) Los órganos a los que corresponda la custodia y archivo de documentos.

c) Los órganos que hayan previsto sus normas de competencia.

d) Las oficinas de asistencia en materia de registros, respecto de los documentos originales o copias auténticas presentados por las personas interesadas para que se remitan desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. La expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original, podrá llevarse a cabo mediante actuación administrativa automatizada o por personal funcionario habilitado inscrito en el Registro de Funcionarios Habilitados de la Administración General del Estado al que se refiere el artículo 31 de este Reglamento.

3. Los titulares de los órganos que se relacionan en los párrafos a), b) c) y d) del apartado 1 de este artículo designarán a los funcionarios y funcionarias habilitados para la emisión de las copias electrónicas auténticas, que se llevará a cabo mediante el correspondiente proceso de digitalización.

Artículo 49. *Emisión de copias de documentos aportados en papel por el interesado.*

Cuando el interesado presente en papel una copia de un documento público administrativo o de un documento privado para incorporarlo a un expediente administrativo,

el proceso de digitalización por la Administración Pública generará una copia electrónica que tendrá el mismo valor que la copia presentada en papel.

Artículo 50. *Referencia temporal de los documentos administrativos electrónicos.*

1. Todos los documentos administrativos electrónicos deberán llevar asociadas una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

a) Marca de tiempo, entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

b) Sello electrónico cualificado de tiempo, entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador cualificado de servicios de confianza que asegure la exactitud e integridad de la marca de tiempo del documento. Los sellos electrónicos de tiempo no cualificados serán asimilables a todos los efectos a las marcas de tiempo.

2. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello electrónico cualificado de tiempo

La información relativa a las marcas y sellos electrónicos cualificados de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad y normativa correspondiente.

3. La relación de prestadores cualificados de servicios de confianza que prestan servicios de sellado de tiempo en el sector público deberá estar incluida en la «Lista de confianza de prestadores cualificados de servicios de confianza».

Artículo 51. *Configuración del expediente administrativo electrónico.*

1. El foliado de los expedientes administrativos electrónicos se llevará a cabo mediante un índice electrónico autenticado que garantizará la integridad del expediente y permitirá su recuperación siempre que sea preciso.

2. Un mismo documento electrónico podrá formar parte de distintos expedientes administrativos.

3. El índice electrónico autenticado será firmado por el titular del órgano que conforme el expediente para su tramitación o bien podrá ser sellado electrónicamente en el caso de expedientes electrónicos que se formen de manera automática, a través de un sistema que garantice su integridad.

Artículo 52. *Ejercicio del derecho de acceso al expediente electrónico y obtención de copias de los documentos electrónicos.*

De acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/2015, de 1 de octubre, el derecho de acceso de las personas interesadas que se relacionen electrónicamente con las Administraciones Públicas al expediente electrónico y, en su caso, a la obtención de copia total o parcial del mismo, se entenderá satisfecho mediante la puesta a disposición de dicho expediente en el Punto de Acceso General electrónico de la Administración competente o en la sede electrónica o sede electrónica asociada que corresponda.

A tal efecto, la Administración destinataria de la solicitud remitirá al interesado o, en su caso a su representante, la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición, garantizando aquella el acceso durante el tiempo que determine la correspondiente política de gestión de documentos electrónicos siempre de acuerdo con el dictamen de valoración emitido por la autoridad calificadora correspondiente, y el cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal y de transparencia y acceso a la información pública y de patrimonio documental, histórico y cultural.

Artículo 53. *Tiempo de conservación y destrucción de documentos.*

1. Los documentos presentados por el interesado en soporte papel que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez digitalizados serán conservados a su disposición durante seis meses para que pueda

recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

2. Los documentos presentados por el interesado en formato electrónico dentro de un dispositivo, que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez incorporados al expediente serán conservados a su disposición durante seis meses para que pueda recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

3. Transcurrido el plazo previsto en los apartados anteriores, la destrucción de los documentos se realizará de acuerdo con las competencias del Ministerio de Cultura y Deporte o del órgano competente de la comunidad autónoma, y siempre que no se trate de documentos con valor histórico, artístico u otro relevante o de documentos en los que la firma u otras expresiones manuscritas o mecánicas confieran al documento un valor especial.

4. Cuando la generación de copias electrónicas auténticas se realice a partir de documentos originales o copias auténticas de documentos en soporte no electrónico que se conserven formando parte de sus correspondientes expedientes y series documentales en cualesquiera de las oficinas, archivos o dependencias de cualquier organismo de las Administraciones públicas, dichos documentos originales o copias auténticas de documentos en soporte no electrónico se restituirán a sus oficinas, archivos o dependencias de origen, donde les será de aplicación la normativa específica en materia de archivos y conservación del patrimonio documental en su respectivo ámbito y siguiendo lo establecido por las autoridades calificadoras que correspondan.

5. En el ámbito estatal, se estará a lo preceptuado en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y entidades de derecho público y la conservación de documentos administrativos en soporte distinto al original.

CAPÍTULO II

Archivo electrónico de documentos

Artículo 54. *Conservación de documentos electrónicos.*

1. De acuerdo con lo previsto en el artículo 46 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, así como sus organismos públicos y entidades de derecho público vinculados o dependientes, deberán conservar en soporte electrónico todos los documentos que formen parte de un expediente administrativo y todos aquellos documentos con valor probatorio creados al margen de un procedimiento administrativo.

La copia electrónica auténtica generada conforme a lo dispuesto en el artículo 27 de la Ley 39/2015, de 1 de octubre, tiene la consideración de patrimonio documental a efectos de aplicación de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español o la normativa autonómica correspondiente, siendo el periodo de conservación de los documentos el establecido por las autoridades calificadoras que correspondan.

2. Cada Administración Pública, regulará los períodos mínimos de conservación de los documentos electrónicos, que formen parte del expediente de un procedimiento cuya tramitación haya concluido, conforme a su normativa específica de archivos y patrimonio documental.

Cuando se tenga conocimiento por la Administración Pública, organismo o entidad de la existencia de procedimientos judiciales que afecten o puedan afectar a documentos electrónicos, estos deberán conservarse a disposición de los órganos jurisdiccionales, hasta tanto exista constancia de la terminación del procedimiento judicial correspondiente en las sucesivas instancias, por haber recaído resolución no susceptible de recurso o procedimiento alguno ante órganos jurisdiccionales nacionales o internacionales.

3. La conservación de los documentos electrónicos deberá realizarse de forma que permita su acceso y comprenda, como mínimo, su identificación, contenido, metadatos, firma, estructura y formato.

También será posible la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos, así como para la comprobación de la identificación o firma electrónica de dichos datos.

Los plazos de conservación de esta información están sujetos a los mismos plazos establecidos para los correspondientes documentos electrónicos.

4. Para asegurar la conservación, acceso y consulta de los documentos electrónicos archivados con independencia del tiempo transcurrido desde su emisión, se podrán trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones, de acuerdo con lo previsto en el artículo 27 de la Ley 39/2015, de 1 de octubre y en la normativa específica de archivos y patrimonio documental, histórico y cultural.

Asimismo, se planificarán las actuaciones de preservación digital que garanticen la conservación a largo plazo de los documentos digitales y permitan de esta forma dar cumplimiento a lo establecido en el párrafo anterior

5. En todo caso, bajo la supervisión de los responsables de la seguridad y de los responsables de la custodia y gestión del archivo electrónico y de los responsables de las unidades productoras de la documentación se establecerán los planes y se habilitarán los medios tecnológicos para la migración de los datos a otros formatos y soportes que permitan garantizar la autenticidad, integridad, disponibilidad, conservación y acceso al documento cuando el formato de los mismos deje de figurar entre los admitidos por el Esquema Nacional de Interoperabilidad y normativa correspondiente.

Artículo 55. *Archivo electrónico único.*

1. El archivo electrónico único de cada Administración es el conjunto de sistemas y servicios que sustenta la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos administrativos o actuaciones correspondientes.

2. En el archivo electrónico único de la Administración General del Estado serán accesibles todos los documentos y expedientes electrónicos del sector público estatal una vez finalizados los procedimientos y en los plazos determinados por la Comisión Superior Calificadora de Documentos Administrativos de acuerdo con lo que se desarrolle reglamentariamente.

La gestión del archivo electrónico único garantizará la autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia de los expedientes y documentos almacenados, así como su acceso, en las condiciones exigidas por el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad, por la normativa de transparencia, acceso a la información pública y buen gobierno, por la legislación de archivos y patrimonio histórico y cultural y por la normativa específica que sea de aplicación, de acuerdo con lo que se desarrolle reglamentariamente.

TÍTULO IV

De las relaciones y colaboración entre las Administraciones Públicas para el funcionamiento del sector público por medios electrónicos

CAPÍTULO I

Colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos

Artículo 56. *Relaciones interadministrativas e interorgánicas por medios electrónicos.*

De acuerdo con lo previsto en el artículo 3.2 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, en el ejercicio de sus competencias, estarán obligadas a

relacionarse a través de medios electrónicos entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

Artículo 57. *Comunicaciones en la Administración General del Estado.*

Los órganos de la Administración General del Estado y los organismos públicos y entidades de derecho público vinculados o dependientes de esta deberán utilizar medios electrónicos para comunicarse entre sí.

Las comunicaciones se efectuarán a través del Registro Electrónico General de la Administración General del Estado o registro del organismo público o entidad de derecho público de que se trate, o por cualquier otro medio electrónico que permita dejar constancia de su recepción.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

Artículo 58. *Adhesión a sedes electrónicas y sedes electrónicas asociadas.*

Las Administraciones Públicas y los organismos públicos y entidades de derecho público vinculados o dependientes podrán adherirse voluntariamente, mediante la formalización del correspondiente instrumento de adhesión, a las sedes electrónicas o sedes asociadas disponibles de titularidad de la misma Administración u otra Administración Pública, sin que se constituya como sede electrónica asociada.

Artículo 59. *Adhesión a la Carpeta Ciudadana del sector público estatal.*

Las Administraciones Públicas podrán integrar sus respectivas áreas personalizadas o carpetas ciudadanas a que se refiere el segundo párrafo del artículo 7.3 de este Reglamento, si las hubiere, o determinadas funcionalidades de las mismas, con la Carpeta Ciudadana prevista en el artículo 8 de este Reglamento, de forma que el interesado pueda acceder a sus contenidos o funcionalidades mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos de carácter personal, independientemente de cuál haya sido su punto de acceso.

Artículo 60. *Sistema de interconexión de Registros.*

1. Las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de cada Administración, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán ser interoperables.

2. Las interconexiones entre Registros de las Administraciones Públicas deberán realizarse a través del Sistema de Interconexión de Registros (SIR) gestionado por el Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en la correspondiente Norma Técnica.

3. En el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de la Administración General del Estado, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán permitir la interoperabilidad con los sistemas de gestión de expedientes de las unidades de tramitación correspondientes.

Artículo 61. *Transmisiones de datos.*

1. Las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015, de 1 de octubre, realizadas a través de redes corporativas de las Administraciones Públicas para el envío de documentos elaborados por cualquier Administración, mediante consulta a las

plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, tienen la consideración de certificados administrativos necesarios para el procedimiento o actuación administrativa.

2. Cuando las personas interesadas no aporten datos y/o documentos que ya obren en poder de las Administraciones Públicas, de conformidad con lo establecido en la Ley 39/2015, de 1 de octubre, se seguirán las siguientes reglas:

a) Si el órgano administrativo encargado de la tramitación del procedimiento, puede acceder electrónicamente a los datos, documentos o certificados necesarios mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, los incorporará al procedimiento administrativo correspondiente. Quedará constancia en los ficheros del órgano, organismo público o entidad de derecho público cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario.

b) Excepcionalmente, en caso de que no se pueda realizar el acceso electrónico a los datos mediante la consulta a que se refiere la letra anterior, se podrá solicitar por otros medios habilitados al efecto y se conservará la documentación acreditativa de la circunstancia que imposibilitó dicho acceso electrónico, incorporándola al expediente.

3. Toda transmisión de datos se efectuará a solicitud del órgano o entidad tramitadora en la que se identificarán los datos requeridos y sus titulares, así como la finalidad para la que se requieren. Además, si en la petición de datos interviene un empleado o empleada público se incluirá la identificación de este en la petición.

4. El órgano, organismo público o entidad de derecho público cesionario será responsable del correcto acceso electrónico a los datos cuya titularidad corresponda a otro órgano, organismo público o entidad de derecho público, así como de su utilización, en particular, cuando los datos a los que se accede tengan un régimen de especial protección. Asimismo, cuando para dicho acceso se requiera el consentimiento del interesado, el cesionario será responsable del requerimiento de dicho consentimiento.

5. La cesión de datos dentro de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada, entendiéndose por tal la consulta realizada íntegramente a través de medios telemáticos en la que no haya intervenido de forma directa un empleado o empleada público.

6. Las transmisiones de datos que se realicen en virtud del artículo 14 del Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012 no requerirán previsualización de los datos por parte del usuario o usuaria solicitante para proceder a su uso por parte del órgano o entidad tramitadora.

Artículo 62. *Plataformas de intermediación de datos.*

1. Las plataformas de intermediación de datos dejarán constancia de la fecha y hora en que se produjo la transmisión, así como del procedimiento administrativo, trámite o actuación al que se refiere la consulta. Las plataformas de intermediación, o sistema electrónico equivalente, existentes en el sector público deberán ser interoperables con la Plataforma de Intermediación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes y entre ellas.

La adhesión a las plataformas de intermediación de datos requerirá que se garantice el cumplimiento de las condiciones de seguridad exigidas por los cedentes de la información para el tratamiento de datos por parte de la plataforma encargada del tratamiento de dichos datos y de los cesionarios de los mismos.

2. En el ámbito estatal, se dispondrá de la Plataforma de Intermediación de Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes a que se refiere la Ley 39/2015, de 1 de octubre. Dicha Plataforma será gestionada la Secretaría General de Administración Digital y actuará como un punto a través del cual cualquier órgano, organismo público o entidad de derecho público podrá consultar los datos o documentos asociados al procedimiento de que se trate, con

independencia de que la presentación de los citados datos o documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate.

3. La Plataforma de Intermediación de la Administración General del Estado actuará como punto de conexión con el sistema técnico regulado por el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, para el intercambio automático de datos o documentos a nivel europeo.

Artículo 63. *Remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición.*

1. Cuando desde una Administración Pública se solicite a otra un expediente electrónico, la remisión por esta, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición de la primera equivaldrá a la remisión del mismo, siempre que se garantice la integridad del acceso a lo largo del tiempo que determine la correspondiente política de gestión de documentos electrónicos y el cumplimiento de la normativa de interoperabilidad aplicable al tipo de expediente.

2. El mismo procedimiento previsto en el apartado anterior se podrá utilizar cuando la solicitud se produzca dentro del ámbito de una misma Administración Pública.

CAPÍTULO II

Transferencia y uso compartido de tecnologías entre Administraciones Públicas

Artículo 64. *Reutilización de sistemas y aplicaciones de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 157 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por estar previsto en una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. A tal efecto, de acuerdo con lo previsto en el artículo 158 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización en modo producto o en modo servicio, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad.

Estos directorios deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, con el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización previsto en el artículo 17 del Real Decreto 4/2010, de 8 de enero.

3. Las condiciones de licenciamiento de los sistemas y aplicaciones de las Administraciones públicas y el uso y funcionamiento de los directorios de aplicaciones reutilizables deberán ajustarse a lo previsto en el Real Decreto 4/2010, de 8 de enero.

4. Las Administraciones públicas procurarán la construcción de aplicaciones reutilizables, bien en modo producto o en modo servicio, con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia y para atender de forma efectiva las solicitudes recibidas en virtud del artículo 157 de la Ley 40/2015, de 1 de octubre.

5. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

Las conclusiones con respecto al resultado de dicha consulta al directorio general se incorporarán en el expediente de contratación y reflejarán, en su caso, que no existen

soluciones disponibles para su reutilización que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir.

En el caso de existir una solución disponible para su reutilización total o parcial, la justificación de la no reutilización se realizará en términos de eficiencia conforme a lo establecido en el artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Artículo 65. *Adhesión a las plataformas de la Administración General del Estado.*

1. La adhesión al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado prevista en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento, así como a aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en estas normas se realizará mediante adhesión por el órgano competente de la Administración Pública que corresponda, en el que se dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

A tal efecto, los modelos de adhesión a las plataformas, registros o servicios, que incluirán los términos de prestación del servicio y de la contribución al sostenimiento del mismo, se aprobarán mediante Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital o, en su caso, del órgano directivo, organismo público o entidad de derecho público que sea competente de las plataformas, registros o servicios de que se trate.

2. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación. Si la plataforma provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o de distinta plataforma, la autenticación de la entidad solicitante puede acreditarse, ante la entidad cedente, mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma en cuestión de la que es usuaria la entidad solicitante, que actuará en nombre de los órganos y organismos o entidades adheridos que actúan como solicitantes.

La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

3. Los órganos competentes para la gestión del procedimiento administrativo de las Administraciones que se adhieran a estas plataformas, registros o servicios electrónicos se responsabilizarán del uso que hagan de las mismas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de que una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, y sin perjuicio de la ampliación de plazos a que se refiere el artículo 32.4 de la Ley 39/2015, de 1 de octubre, cada Administración pública será responsable de la continuación de la tramitación de sus procedimientos administrativos y servicios a la ciudadanía.

4. La adhesión de las comunidades autónomas o entidades locales a las plataformas estatales o registros previstos en la disposición adicional segunda de la Ley 39/2015, de 1 de octubre, es voluntaria, si bien la no adhesión deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, para lo que se enviará el correspondiente informe al Ministerio de Asuntos Económicos y Transformación Digital, en el que deberá incluirse la justificación del cumplimiento de los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, de plataformas, registros o servicios electrónicos que se utilicen, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes plataformas.

Disposición adicional primera. *Obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado.*

Las personas participantes en procesos selectivos convocados por la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes a la misma, deberán realizar la presentación de las solicitudes y documentación y, en su caso, la subsanación y los procedimientos de impugnación de las actuaciones de estos procesos selectivos a través de medios electrónicos.

Disposición adicional segunda. *Formación de empleados y empleadas públicos de la Administración General del Estado.*

La Administración General del Estado promoverá la formación del personal a su servicio para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública, establecido en la Ley 39/2015, de 1 de octubre.

Disposición adicional tercera. *Nodo de interoperabilidad de identificación electrónica del Reino de España.*

1. Se crea el nodo de interoperabilidad de identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre los Estados miembros, de acuerdo con lo previsto en el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
2. El nodo de interoperabilidad de identificación electrónica del Reino de España se gestionará por el Ministerio de Asuntos Económicos y Transformación Digital.
3. Las entidades pertenecientes al sector público deberán definir y publicar en su sede electrónica el nivel de seguridad en la identificación electrónica exigido en los procedimientos y servicios que gestionan, de acuerdo con el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014. Este nivel de seguridad en la identificación electrónica del sistema de información que soporta el procedimiento o servicio se determinará sobre la base del análisis de riesgos, de acuerdo con el Esquema Nacional de Seguridad y normativa correspondiente.
4. Las entidades pertenecientes al sector público deberán admitir en todo caso, en el acceso electrónico a sus procedimientos y servicios los esquemas de identificación notificados por otros Estados Miembros al amparo del Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, siempre que se den estas dos condiciones:

a) El esquema de identificación utilizado tenga un nivel de seguridad en la identificación electrónica sustancial o alto.
b) El nivel de seguridad de dicho esquema sea igual o superior al nivel de seguridad exigido por el procedimiento o servicio de acuerdo con el apartado 3.

Disposición adicional cuarta. *Adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado en el ejercicio de potestades administrativas a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables.*

De acuerdo con lo previsto en el artículo 2.2.b) de la Ley 39/2015, de 1 de octubre, y el artículo 2.2.b) de la Ley 40/2015, de 1 de octubre, cuando las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado ejerzan potestades administrativas y, en consecuencia, les sea de aplicación este Reglamento, se observarán las siguientes disposiciones:

a) De acuerdo con lo previsto en el artículo 58, las entidades de derecho privado tendrán que adherirse a la sede electrónica asociada del ministerio con el que mantengan la vinculación o dependencia o, en su caso, a la sede electrónica o sede electrónica asociada del organismo de derecho público con el que mantengan la misma, en ambos casos mediante la formalización del correspondiente instrumento de adhesión.

Las personas interesadas obligadas a relacionarse electrónicamente con las entidades de derecho privado en el ejercicio de dichas potestades realizarán los trámites del procedimiento mediante los modelos normalizados que estarán disponibles en la sede electrónica asociada o, en su caso, sede electrónica a la que se haya adherido la entidad. El mismo régimen se aplicará a los sujetos no obligados que hayan optado por medios electrónicos de acuerdo con lo previsto en el artículo 3 de este Reglamento.

b) Según lo previsto en los artículos 20.2 y 22.4, mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinarán reglamentariamente los medios admitidos para la firma electrónica en los procedimientos tramitados en el ejercicio de potestades administrativas por parte de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado.

c) De conformidad con lo previsto en el artículo 42, las notificaciones electrónicas que las entidades de derecho privado tengan que practicar se llevarán a cabo en la misma forma que el responsable de la sede electrónica asociada o sede electrónica a la que esté adherida la entidad haya dispuesto para sus propias notificaciones.

Disposición adicional quinta. *Adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado.*

1. Sin perjuicio de lo previsto en el artículo 65 de este Reglamento, los órganos constitucionales podrán adherirse al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado y aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento.

2. La adhesión se realizará mediante un acuerdo o acto de adhesión en el que la autoridad competente de las instituciones u órganos anteriores dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

Para el estudio de su viabilidad, remitirá con carácter previo al Ministerio al que pertenezca el órgano titular de la plataforma o servicio una memoria justificativa y económica en que se explicite el volumen de trámites que estaría previsto realizar a través de la plataforma, el registro o servicio electrónico de que se trate, los efectos presupuestarios y económicos y cualquier otra razón de interés general que justifique su adhesión.

3. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación.

Si la plataforma, registro o servicio electrónico provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o distinta plataforma, la autenticación de la entidad solicitante puede acreditarse ante la entidad cedente mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma.

4. La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

5. Los órganos competentes en las instituciones u órganos adheridos se responsabilizarán del uso que hagan de las plataformas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, los órganos competentes en las instituciones u órganos adheridos serán responsables de la continuación de la tramitación de sus procedimientos administrativos.

Disposición adicional sexta. *Situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a la entrada en vigor de este real decreto.*

1. En aplicación de lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas existentes en la Administración General del Estado en la fecha de entrada en vigor de este real decreto pasan a tener naturaleza de sedes electrónicas

asociadas de la sede electrónica de la Administración General del Estado, que es la sede del Punto de Acceso General electrónico (PAGe) de la Administración General del Estado, sin necesidad de modificar su instrumento de creación. Las subsedes electrónicas existentes en la fecha de entrada en vigor de este real decreto pasarán también a tener naturaleza de sedes electrónicas asociadas.

2. Las sedes electrónicas de los organismos públicos o entidades de derecho público vinculados o dependientes existentes en la fecha de entrada en vigor de este real decreto mantendrán su naturaleza de sede electrónica. Las subsedes electrónicas de estos pasarán a tener naturaleza de sedes electrónicas asociadas.

Disposición adicional séptima. *Interoperabilidad de los registros electrónicos de apoderamientos.*

1. En aplicación de lo previsto en el artículo 6 de la Ley 39/2015, de 1 de octubre, y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, la Norma Técnica de Interoperabilidad establecerá el modelo de datos y las condiciones de interoperabilidad de los registros electrónicos de apoderamientos, abordando los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, a los registros mercantiles, de la propiedad y a los protocolos notariales.

2. En el ámbito de la Administración General del Estado, el cumplimiento de las previsiones del artículo 33.2 del Reglamento sobre el acceso al Registro Electrónico de Apoderamientos de la Administración General del Estado está vinculado a la aprobación y aplicación de la Norma Técnica a que se refiere el apartado 1 anterior.

Disposición adicional octava. *Supletoriedad en Registro Civil.*

De conformidad con lo dispuesto en el artículo 88 y en la Disposición final primera de la Ley 20/2011, de 21 de julio, del Registro Civil, este Reglamento será de aplicación supletoria en lo no previsto en dicha Ley y su normativa de desarrollo específica, en cuanto a todo lo relacionado con la tramitación administrativa de los procedimientos específicos de Registro Civil.

Disposición adicional novena. *Autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre.*

1. Los sistemas de identificación a que se refiere el artículo 9.2.c) y los sistemas de firma a que se refiere el artículo 10.2.c) de la ley 39/2015, de 1 de octubre, que, en ambos casos, se hubieran puesto en servicio hasta el 6 de noviembre de 2019, fecha de entrada en vigor de la modificación de dichos artículos en virtud del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, no requerirán la autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior, siempre y cuando no hayan sido modificados tras dicha fecha.

2. Los sistemas que, tras el 6 de noviembre de 2019, hayan sido autorizados en aplicación de las previsiones de los artículos 9.2.c) y 10.2.c) de la Ley 39/2015, de 1 de octubre, y sean modificados posteriormente, deberán ser objeto de una nueva autorización previa a su puesta en servicio.

Disposición adicional décima. *Especialidades por razón de materia.*

1. De acuerdo con la disposición adicional primera de la Ley 39/2015, de 1 de octubre, los procedimientos administrativos regulados en leyes especiales por razón de la materia que no exijan alguno de los trámites previstos en la citada ley o regulen trámites adicionales o distintos se regirán, respecto a estos, por lo dispuesto en dichas leyes especiales.

2. Las siguientes actuaciones y procedimientos se regirán por su normativa específica y supletoriamente por lo dispuesto en la Ley 39/2015, de 1 de octubre:

a) Las actuaciones y procedimientos de aplicación de los tributos en materia tributaria y aduanera, así como su revisión en vía administrativa.
b) Las actuaciones y procedimientos de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y desempleo.
c) Las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.
d) Las actuaciones y procedimientos en materia de extranjería y asilo.

3. De acuerdo con lo previsto en la Disposición adicional decimoséptima de la Ley 40/2015, de 1 de octubre, la Agencia Estatal de Administración Tributaria se regirá por su legislación específica y únicamente de forma supletoria y en tanto resulte compatible con su legislación específica por lo previsto en dicha Ley. El acceso, la cesión o la comunicación de información de naturaleza tributaria se regirán en todo caso por su legislación específica.

ANEXO

Definiciones

– Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otras personas usuarias.
– Archivo electrónico único de cada Administración: Conjunto de sistemas y servicios que sustente la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos o actuaciones correspondientes.
– Autenticación: Procedimiento de verificación de la identidad digital de un sujeto en sus interacciones en el ámbito digital, típicamente mediante factores tales como «algo que se sabe»(contraseñas o claves concertadas), «algo que se tiene» sean componentes lógicos (como certificados software) o dispositivos físicos (en expresión inglesa, tokens), o «algo que se es» (elementos biométricos), factores utilizados de manera aislada o combinados.
– Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
– Canal: Estructura o medio de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, etc.).
– Certificado electrónico: Documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con su propietario. Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.
– Certificado cualificado: Un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
– Certificado cualificado de sello electrónico: Certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
– Código malicioso: Tipo de software de carácter dañino que crea o aprovecha vulnerabilidades en dispositivos, sistemas y archivos informáticos que permiten el acceso remoto no autorizado, la generación de puertas traseras, el robo o exfiltración de datos, la destrucción de información, u otras acciones perjudiciales.
– Código Seguro de Verificación (CSV): Código que identifica a un documento electrónico y cuya finalidad es garantizar el origen e integridad de los documentos mediante

el acceso a la sede electrónica correspondiente; el carácter único del código generado para cada documento; su vinculación con el documento generado, de forma que cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente; la posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento; así como un acceso al documento restringido a quien disponga del código seguro de verificación.

– Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Copia auténtica: Tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido

– Copia autorizada electrónica: documento notarial electrónico generado por el notario que autorizó la escritura, con el mismo valor y efectos que la copia en papel y al cual se le atribuye también valor de documento público.

– Digitalización: Proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

– Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones

– Directorio de aplicaciones reutilizables: instrumento que contiene la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

– Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

– Entorno cerrado de comunicación: escenario de comunicaciones delimitado, controlado y protegido en el que los participantes se relacionan a través de medios electrónicos, según unas garantías y condiciones determinadas que incluyen la relación de emisores y receptores autorizados, la naturaleza de los datos a intercambiar y las medidas de seguridad y protección de datos.

– Especificación técnica: Según el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea, documento en el que se prescriben los requisitos técnicos que debe reunir un producto, proceso, servicio o sistema y que establece uno o más de los aspectos siguientes:

• Las características que debe tener un producto, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud y seguridad y sus dimensiones, así como los requisitos aplicables al producto en lo que respecta a la denominación con la que se vende, la terminología, los símbolos, los ensayos y los métodos de ensayo, el embalaje, el marcado o el etiquetado y los procedimientos de evaluación de la conformidad;

• los métodos y procedimientos de producción de los productos agrícolas, definidos en el artículo 38, apartado 1, del TFUE, de los productos destinados a la alimentación humana y animal y de los medicamentos, así como los métodos y procedimientos de producción relacionados con los demás productos, en caso de que estos influyan en sus características;

• las características que debe tener un servicio, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud o seguridad, así como los requisitos aplicables al proveedor en lo que respecta a la información que debe facilitarse a la persona destinataria, tal como se especifica en el artículo 22, apartados 1 a 3, de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior.

• los métodos y los criterios para evaluar el rendimiento de los productos de construcción, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.º

305/2011 del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, por el que se establecen condiciones armonizadas para la comercialización de productos de construcción, en relación con sus características esenciales.

– Esquema Nacional de Interoperabilidad: Instrumento que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

– Esquema Nacional de Seguridad: Instrumento que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

– Expediente administrativo: Conjunto ordenado de documentos y actuaciones relativos a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

– Firma electrónica: Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: La firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS.

– Firma electrónica cualificada: Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Formato de documento: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria. Se corresponde habitualmente con una especificación técnica.

– Identificación: Procedimiento para reconocer de forma única la identidad de un sujeto que culmina tras un registro previo con la asignación de un elemento identificador singular en formato electrónico que representa de forma única a una persona física o jurídica o a una persona física que representa a una persona jurídica para interacción en el entorno digital.

– Infraestructura o servicio común: Capacidad organizativa y técnica que satisface necesidades comunes de las personas usuarias en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

– Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

– Licenciamiento: Condiciones aplicables a la reutilización de cualquier tipo de material en formato electrónico que pueda ser empleado de forma recurrente.

– Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

– Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

– Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

– Nodo de interoperabilidad: Entidad que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que estas fijen.

– Política de firma electrónica: Conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

– Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

– Portal de internet de una Administración Pública: Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

– Prestador de Servicios de Confianza: Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza, según lo previsto en el Reglamento eIDAS.

– Punto de Acceso General: Portal de internet que facilita el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente y aglutina o conduce a las sedes electrónicas asociadas de sus órganos y las sedes electrónicas de sus organismos públicos y entidades de derecho público.

– Sello electrónico: Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

– Sello electrónico avanzado: Sello electrónico que cumple los siguientes requisitos: 1) estar vinculado al creador del sello de manera única; 2) permitir la identificación del creador del sello; 3) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y 4) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

– Sello electrónico cualificado: Sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

– Sede electrónica: Dirección electrónica, disponible para la ciudadanía a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ejercicio de sus competencias.

– Sede electrónica asociada: Sede electrónica disponible para la ciudadanía a través de redes de telecomunicaciones que se crea por razones organizativas o técnicas vinculada a la sede electrónica de una Administración Pública o a la sede electrónica de un organismo público o entidad de derecho público.

– Sello de tiempo: Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento

– Sistema de Interconexión de Registros: Infraestructura básica que permite el intercambio de asientos electrónicos de registro entre las Administraciones Públicas.

– Trazabilidad: Posibilidad de identificar el origen de un documento en las distintas fases de su producción, pudiendo determinar en qué fase y por quién se han producido, en su caso, las modificaciones del documento original.

§ 26

Ley 9/1968, de 5 de abril, sobre secretos oficiales

Jefatura del Estado
«BOE» núm. 84, de 6 de abril de 1968
Última modificación: 11 de octubre de 1978
Referencia: BOE-A-1968-444

Es principio general, aun cuando no esté expresamente declarado en nuestras Leyes Fundamentales, la publicidad de la actividad de los Órganos del Estado, porque las cosas públicas que a todos interesan pueden y deben ser conocidas de todos.

Este principio de publicidad en mayor o menor extensión, se halla regulado en lo que concierne a los debates e interpelaciones en las Cortes Españolas y al despacho de los asuntos judiciales, pero, en cambio, sólo de una manera fraccionada tiene su regulación, en lo que atañe a la Administración del Estado, en dispersas disposiciones, entre las que, por su reciente promulgación, pueden citarse la Ley de Prensa (artículo séptimo) y Decreto setecientos cincuenta/mil novecientos sesenta y seis, de treinta y uno de marzo, en las que sólo se contempla la publicidad en el aspecto parcial de la información debida a las publicaciones periódicas y agencias de información. Una regulación suficiente existe en la esfera de la Administración Local.

Mas si la publicidad ha de ser característica de la actuación de los Órganos del Estado, es innegable la necesidad de imponer limitaciones, cuando precisamente de esa publicidad puede derivarse perjuicio para la causa pública, la seguridad del mismo Estado o los intereses de la colectividad nacional.

Destancan por su especial importancia aquellas cuestiones cuyo conocimiento por personas no autorizadas pueda dañar o ponga en riesgo la seguridad del Estado o los intereses fundamentales de la Nación y que constituyen los verdaderos «secretos oficiales», protegidos por sanciones penales que, tanto en el Código Penal Común como en el de Justicia Militar, alcanzan penas de la máxima severidad. Pero esta sanción penal, especialmente represiva, sólo de una manera indirecta, por medio de la intimidación, protege el descubrimiento o revelación de secretos. Las medidas de protección eficaces son las que la propia Administración ha de establecer para garantizar que los documentos o materiales en que físicamente se reflejan los secretos, no puedan ser conocidos más que por aquellas personas que, por razón de su cometido, estén autorizadas para ello.

En este aspecto existe una laguna en nuestra legislación, que, al contrario de lo que ocurre en los Estados caracterizados por la mayor libertad de información, no prevé una regulación de las medidas protectoras de los secretos oficiales Para remediar esta situación, la Ley establece un conjunto de medidas positivas para evitar que trascienda el conocimiento de lo que debe permanecer secreto, señalando normas severas que impidan la generalización de calificaciones que tienen carácter excepcional.

Con la denominación de «materias clasificadas» también utilizada en otros países, se comprenden los dos grados de secretos oficiales generalmente admitidos. La determinación

de las Autoridades y funcionarios que pueden otorgar y levantar las calificaciones, los efectos de cada una de éstas y las líneas generales de las medidas protectoras que habrán de desarrollarse reglamentariamente y con carácter uniforme por todos los servicios afectados, constituyen el contenido fundamental de la Ley, que se completa con un sistema de protección, así como la referencia de las responsabilidades que procedan por infracciones en materia de secretos oficiales.

Asimismo, desde el punto de vista de la seguridad jurídica y de la garantía de los ciudadanos, es importante resaltar que la Ley establece la necesidad de notificar a los medios de información la declaración de «materia clasificada» cuando se prevea que ésta puede llegar a conocimiento de ellos, así como la circunstancia de que conste el hecho de la clasificación para que recaiga sobre los particulares la obligación de colaboración que impone el artículo nueve, uno. Y, en fin, se consagra la expresa admisión de recurso contencioso-administrativo contra las resoluciones sancionadoras que pongan fin a la vía administrativa, sin olvidar por lo demás el importante juego del control político que en esta materia se reconoce a las Cortes Españolas y al Consejo Nacional del Movimiento.

En su virtud, y de conformidad con la Ley aprobada por las Cortes Españolas, vengo en sancionar:

Artículo primero.

Uno. Los Órganos del Estado estarán sometidos en su actividad al principio de publicidad, de acuerdo con las normas que rijan su actuación, salvo los casos en que por la naturaleza de la materia sea ésta declarada expresamente «clasificada», cuyo secreto o limitado conocimiento queda amparado por la presente Ley.

Dos. Tendrán carácter secreto, sin necesidad de previa clasificación, las materias así declaradas por Ley.

Artículo segundo.

A los efectos de esta Ley podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado.

Artículo tercero.

Las «materias clasificadas» serán calificadas en las categorías de secreto y reservado en atención al grado de protección que requieran.

Artículo cuarto.

La calificación a que se refiere el artículo anterior corresponderá exclusivamente, en la esfera de su competencia, al Consejo de Ministros y a la Junta de Jefes de Estado Mayor.

Artículo quinto.

La facultad de calificación a que se refiere el artículo anterior no podrá ser transferida ni delegada.

Artículo sexto.

El personal de la Administración del Estado o de las Fuerzas Armadas que tenga conocimiento de cualquier asunto que, a su juicio, reúna las condiciones del artículo segundo, deberá hacerlo llegar a alguno de los órganos comprendidos en el artículo cuarto en la forma que reglamentariamente se determine.

Artículo séptimo.

La cancelación de cualquiera de las calificaciones previstas en el artículo tercero de esta Ley será dispuesta por el órgano que hizo la respectiva declaración.

Artículo octavo.

Las calificaciones de secreto o reservado, hechas con arreglo a los términos de la presente Ley y de las disposiciones que reglamentariamente se dicten para su aplicación, determinarán, entre otros, los siguientes efectos:

A) Solamente podrán tener conocimiento de las "materias clasificadas" los órganos y las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen.

B) La prohibición de acceso y las limitaciones de circulación a personas no autorizadas en locales, lugares o zonas en que radiquen las «materias clasificadas».

C) El personal que sirva en la Administración del Estado y en las Fuerzas Armadas estará obligado a cumplir cuantas medidas se hallen previstas para proteger las «materias clasificadas».

Artículo noveno.

Uno. La persona a cuyo conocimiento o poder llegue cualquier «materia clasificada», conforme a esta Ley, siempre que le conste esta condición, está obligada a mantener el secreto y entregarla a la Autoridad civil o militar más cercana y, si ello no fuese posible, a poner en conocimiento de ésta su descubrimiento o hallazgo. Esta Autoridad lo comunicará sin dilación al Departamento ministerial que estime interesado o a la Presidencia del Gobierno, adoptando entretanto las medidas de protección que su buen juicio le aconseje.

Dos. Cuando una «materia clasificada» permita prever que pueda llegar a conocimiento de los medios de información, se notificará a éstos la calificación de secreto o reservado.

Artículo diez.

Uno. Las calificaciones a que se refiere el artículo cuarto, en cualquiera de sus grados, se conferirán mediante un acto formal y con los requisitos y materializaciones que reglamentariamente se determinen.

Dos. La declaración de "materias clasificadas" no afectará al Congreso de los Diputados ni al Senado, que tendrán siempre acceso a cuanta información reclamen, en la forma que determinen los respectivos Reglamentos y, en su caso, en sesiones secretas.

Tres. Las «materias clasificadas» llevarán consigo una anotación en la que conste esta circunstancia y la calificación que les corresponda conforme al artículo tercero.

Cuatro. Las copias o duplicados de una «materia clasificada» tendrán el mismo tratamiento y garantía que el original y sólo se obtendrán previa autorización especial y bajo numeración.

Artículo once.

Uno. Las personas facultadas para tener acceso a una «materia clasificada» quedarán obligadas a cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen, así como las particulares que para cada caso concreto puedan establecerse.

Dos. Corresponde a los órganos señalados en el artículo cuarto conceder en sus respectivas dependencias las autorizaciones para el acceso a las "materias clasificadas", así como para su desplazamiento fuera de las mismas.

Tres. A toda persona que tenga acceso a una «materia clasificada» se le hará saber la índole de la misma con las prevenciones oportunas.

Artículo doce.

Los órganos referidos en el artículo cuarto atenderán al mantenimiento y mejora de los sistemas de protección y velarán por el efectivo cumplimiento de cuanto se dispone en la presente Ley y en especial por la correcta aplicación de las calificaciones de secreto o reservado y porque se promuevan las acciones penales, las medidas disciplinarias y los expedientes administrativos para corregir las infracciones a esta Ley.

Artículo trece.

Las actividades reservadas por declaración de Ley y las "materias clasificadas" no podrán ser comunicadas, difundidas ni publicadas, ni utilizado su contenido fuera de los límites establecidos por la Ley. El incumplimiento de esta limitación será sancionado, si procediere, conforme a las Leyes penales, y por vía disciplinaria, en su caso, considerándose en este último supuesto la infracción como falta muy grave.

Artículo catorce.

La calificación de secreto o reservado no impedirá el exacto cumplimiento de los trámites de audiencia, alegaciones, notificaciones directas a los interesados, sin perjuicio de la eventual aplicación de las sanciones previstas en esta Ley en caso de violación del secreto por parte de los interesados.

DISPOSICIÓN FINAL

En Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armadas, se regularán los procedimientos y medidas necesarios para la aplicación de la presente Ley y protección de las «materias clasificadas».

Se determinará igualmente con todo el detalle necesario y con especificación de las medidas técnicas precisas el régimen de custodia, traslado, registro, archivo, examen y destrucción de las materias clasificadas, así como la elaboración de copias o duplicados de tales materias.

También se dispondrá lo necesario para que el personal de la Administración Civil del Estado y de las Fuerzas Armadas se halle debidamente instruido en cuestiones de seguridad y protección de secretos.

§ 27

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 31 de marzo de 2021
Referencia: BOE-A-2010-1331

I

La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el ámbito de las Administraciones públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas. Esta obligación tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, así como la remoción de los obstáculos que impidan o dificulten el ejercicio pleno del principio de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías de la información y las comunicaciones, garantizando con ello la independencia en la elección de las alternativas tecnológicas por los ciudadanos, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado. La interoperabilidad se recoge dentro del principio de cooperación en el artículo 4 y tiene un protagonismo singular en el título cuarto dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En dicho título el aseguramiento de la interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones públicas figura en el artículo 40 entre las funciones del órgano de cooperación en esta materia, el Comité Sectorial de Administración Electrónica. A continuación, el artículo 41 se refiere a la aplicación por parte de las Administraciones públicas de las medidas informáticas, tecnológicas y organizativas, y de

seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica. Y, seguidamente, el artículo 42.1 crea el Esquema Nacional de Interoperabilidad que comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad, entre éstas y con los ciudadanos.

La finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

II

El Esquema Nacional de Interoperabilidad tiene presentes las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos, así como en su caso y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre acceso electrónico de los ciudadanos a los servicios públicos, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, accesibilidad, uso de lenguas oficiales, reutilización de la información en el sector público y órganos colegiados responsables de la administración electrónica. Se han tenido en cuenta otros instrumentos, tales como el Esquema Nacional de Seguridad, desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio, o antecedentes como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades.

En términos de las recomendaciones de la Unión Europea se atiende al Marco Europeo de Interoperabilidad, elaborado por el programa comunitario IDABC, así como a otros instrumentos y actuaciones elaborados por este programa y que inciden en alguno de los múltiples aspectos de la interoperabilidad, tales como el Centro Europeo de Interoperabilidad Semántica, el Observatorio y Repositorio de Software de Fuentes Abiertas y la Licencia Pública de la Unión Europea. También se atiende a la Decisión 922/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas, a los planes de acción sobre administración electrónica en materia de interoperabilidad y de aspectos relacionados, particularmente, con la política comunitaria de compartir, reutilizar y colaborar.

III

Este real decreto se limita a establecer los criterios y recomendaciones, junto con los principios específicos necesarios, que permitan y favorezcan el desarrollo de la interoperabilidad en las Administraciones públicas desde una perspectiva global y no fragmentaria, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, en el ámbito de la Ley 11/2007, de 22 de junio, al objeto de conseguir un común denominador normativo.

En consecuencia, el Esquema Nacional de Interoperabilidad atiende a todos aquellos aspectos que conforman de manera global la interoperabilidad. En primer lugar, se atiende a las dimensiones organizativa, semántica y técnica a las que se refiere el artículo 41 de la Ley 11/2007, de 22 de junio; en segundo lugar, se tratan los estándares, que la Ley 11/2007, de 22 de junio, pone al servicio de la interoperabilidad así como de la independencia en la elección de las alternativas tecnológicas y del derecho de los ciudadanos a elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas; en tercer lugar, se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral; en cuarto lugar, se trata la reutilización, aplicada a las aplicaciones

de las Administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz «compartir» se encuentra presente en la definición de interoperabilidad recogida en la Ley 11/2007, de 22 de junio, y junto con «reutilizar», ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar; en quinto lugar, se trata la interoperabilidad de la firma electrónica y de los certificados; por último, se atiende a la conservación, según lo establecido en la citada Ley 11/2007,de 22 de junio, como manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.

En esta norma se hace referencia a la interoperabilidad como un proceso integral, en el que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

La norma se estructura en doce capítulos, cuatro disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria, tres disposiciones finales y un anexo conteniendo el glosario de términos.

El Esquema Nacional de Interoperabilidad se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42, apartado 3, y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Interoperabilidad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

Artículo 2. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el Glosario de Términos incluido en el anexo.

Artículo 3. *Ámbito de aplicación.*

1. El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.
2. El Esquema Nacional de Interoperabilidad y sus normas de desarrollo, prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Interoperabilidad.*

La aplicación del Esquema Nacional de Interoperabilidad se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes principios específicos de la interoperabilidad:

a) La interoperabilidad como cualidad integral.
b) Carácter multidimensional de la interoperabilidad.
c) Enfoque de soluciones multilaterales.

Artículo 5. *La interoperabilidad como cualidad integral.*

La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

Artículo 6. *Carácter multidimensional de la interoperabilidad.*

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones públicas y en la publicación y reutilización de las aplicaciones de las Administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

Artículo 7. *Enfoque de soluciones multilaterales.*

Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas del escalado, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

CAPÍTULO III

Interoperabilidad organizativa

Artículo 8. *Servicios de las Administraciones públicas disponibles por medios electrónicos.*

1. Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables. Estas condiciones deberán en todo caso resultar conformes a los principios, derechos y obligaciones contenidos en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de

desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se potenciará el establecimiento de convenios entre las Administraciones públicas emisoras y receptoras y, en particular, con los nodos de interoperabilidad previstos en el apartado 3 de este artículo, con el objetivo de simplificar la complejidad organizativa sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el Comité Sectorial de Administración electrónica se identificarán, catalogarán y priorizarán los servicios de interoperabilidad que deberán prestar las diferentes Administraciones públicas.

2. Las Administraciones públicas publicarán aquellos servicios que pongan a disposición de las demás administraciones a través de la Red de comunicaciones de las Administraciones públicas españolas, o de cualquier otra red equivalente o conectada a la misma que garantice el acceso seguro al resto de administraciones.

3. Las Administraciones públicas podrán utilizar nodos de interoperabilidad, entendidos como entidades a las cuales se les encomienda la gestión de apartados globales o parciales de la interoperabilidad organizativa, semántica o técnica.

Artículo 9. *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.

CAPÍTULO IV

Interoperabilidad semántica

Artículo 10. *Activos semánticos.*

1. Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes, que serán de preferente aplicación para los intercambios de información en las Administraciones públicas, de acuerdo con el procedimiento establecido en disposición adicional primera.

2. Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes, establecerán y publicarán los correspondientes modelos de datos de intercambio que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

3. Los modelos de datos a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y se publicarán, junto con las definiciones y codificaciones asociadas, a través del Centro de Interoperabilidad Semántica de la Administración, según las condiciones de licenciamiento previstas en el artículo 16.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

CAPÍTULO V

Interoperabilidad técnica

Artículo 11. *Estándares aplicables.*

1. Las Administraciones públicas usarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos, al objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

a) Los documentos y servicios de administración electrónica que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, disponibles mediante estándares abiertos.

b) Los documentos, servicios electrónicos y aplicaciones puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

2. En las relaciones con los ciudadanos y con otras Administraciones públicas, el uso en exclusiva de un estándar no abierto sin que se ofrezca una alternativa basada en un estándar abierto se limitará a aquellas circunstancias en las que no se disponga de un estándar abierto que satisfaga la funcionalidad satisfecha por el estándar no abierto en cuestión y sólo mientras dicha disponibilidad no se produzca. Las Administraciones públicas promoverán las actividades de normalización con el fin de facilitar la disponibilidad de los estándares abiertos relevantes para sus necesidades.

3. Para la selección de estándares, en general y, para el establecimiento del catálogo de estándares, en particular, se atenderá a los siguientes criterios:

a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.

b) La definición de estándar abierto establecida en la Ley 11/2007, de 22 de junio, anexo, letra k).

c) Carácter de especificación formalizada.

d) Definición de «coste que no suponga una dificultad de acceso», establecida en el anexo de este real decreto.

e) Consideraciones adicionales referidas a la adecuación del estándar a las necesidades y funcionalidad requeridas; a las condiciones relativas a su desarrollo, uso o implementación, documentación disponible y completa, publicación, y gobernanza del estándar; a las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

4. Para el uso de los estándares complementarios a la selección indicada en el apartado anterior, se tendrá en cuenta la definición de «uso generalizado por los ciudadanos» establecida en el anexo del presente real decreto.

5. En cualquier caso los ciudadanos podrán elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas, o dirigirse a las mismas, siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos. Para facilitar la interoperabilidad con las Administraciones públicas el catálogo de estándares contendrá una relación de estándares abiertos y en su caso complementarios aplicables.

CAPÍTULO VI

Infraestructuras y servicios comunes

Artículo 12. *Uso de infraestructuras y servicios comunes y herramientas genéricas.*

Las Administraciones públicas enlazarán aquellas infraestructuras y servicios que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para facilitar la interoperabilidad y la relación multilateral en el intercambio de información y de servicios entre todas las Administraciones públicas.

CAPÍTULO VII

Comunicaciones de las Administraciones públicas

Artículo 13. *Red de comunicaciones de las Administraciones públicas españolas.*

1. Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán preferentemente la Red de comunicaciones de las Administraciones públicas españolas para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros.

La Red SARA prestará la citada Red de comunicaciones de las Administraciones públicas españolas.

2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera.

Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.

Artículo 15. *Hora oficial.*

1. Los sistemas o aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial, con una precisión y desfase que garanticen la certidumbre de los plazos establecidos en el trámite administrativo que satisfacen.

2. La sincronización de la fecha y la hora se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al Centro Español de Metrología y, cuando sea posible, con la hora oficial a nivel europeo.

CAPÍTULO VIII

Reutilización y transferencia de tecnología

Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.
b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.
c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.
d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.
e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.
f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.
4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.
b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.

Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.
2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.
b) Documentación asociada.
c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.
d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.

CAPÍTULO IX

Firma electrónica y certificados

Artículo 18. *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las reglas de creación

y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.

Artículo 19. *Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación.*

(Suprimido)

Artículo 20. *Plataformas de validación de certificados electrónicos y de firma electrónica.*

1. Las plataformas de validación de certificados electrónicos y de firma electrónica proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones públicas.
2. Proporcionarán, en un único punto de llamada, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas que pueden encontrase en los dominios de dos administraciones diferentes.
3. Potenciarán la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.
4. Incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza.

CAPÍTULO X

Recuperación y conservación del documento electrónico

Artículo 21. *Condiciones para la recuperación y conservación de documentos.*

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.
b) La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.
c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.
d) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.
e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.
f) El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.
g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los

formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

h) La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Artículo 22. *Seguridad.*

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Artículo 23. *Formatos de los documentos.*

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

Artículo 24. *Digitalización de documentos en soporte papel.*

1. La digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:

a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.

b) Nivel de resolución.

c) Garantía de imagen fiel e íntegra.

d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

2. La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

CAPÍTULO XI

Normas de conformidad

Artículo 25. *Sedes y registros electrónicos.*

La interoperabilidad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Interoperabilidad.

Artículo 26. *Ciclo de vida de servicios y sistemas.*

La conformidad con el Esquema Nacional de Interoperabilidad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.

Artículo 27. *Mecanismo de control.*

Cada órgano o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar, de forma efectiva, el cumplimiento del Esquema Nacional de Interoperabilidad.

Artículo 28. *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público de las Administraciones públicas darán publicidad, en las correspondientes sedes electrónicas, a las declaraciones de conformidad y a otros posibles distintivos de interoperabilidad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Interoperabilidad.

CAPÍTULO XII

Actualización

Artículo 29. *Actualización permanente.*

El Esquema Nacional de Interoperabilidad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan.

Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.

Disposición adicional segunda. *Formación.*

El personal de las Administraciones públicas recibirá la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Interoperabilidad, a cuyo fin los órganos responsables dispondrán lo necesario para que esta formación sea una realidad efectiva.

Disposición adicional tercera. *Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.*

(Suprimida)

Disposición adicional cuarta. *Instituto Nacional de Tecnologías de la Comunicación.*

(Suprimida)

Disposición adicional quinta. *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.

Disposición transitoria primera. *Adecuación de sistemas y servicios.*

Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Interoperabilidad de forma que permitan el cumplimiento de lo establecido en la Disposición final tercera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

Si a los doce meses de la entrada en vigor del Esquema Nacional de Interoperabilidad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación, que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

Disposición transitoria segunda. *Uso de medios actualmente admitidos de identificación y autenticación.*

De acuerdo con lo previsto en el artículo 19 de la Ley 11/2007, de 22 de junio, y en la disposición transitoria primera del Real Decreto 1671/2009, de 6 de noviembre, se establece un plazo de adaptación de veinticuatro meses en el que se podrá seguir utilizando los medios actualmente admitidos de identificación y firma electrónica.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones Públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Glosario de términos

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de

documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Coste que no suponga una dificultad de acceso: Precio del estándar que, por estar vinculado al coste de distribución y no a su valor, no impide conseguir su posesión o uso.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Especificación técnica: Una especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Especificación formalizada: Aquellas especificaciones que o bien son normas en el sentido de la Directiva 98/34 o bien proceden de consorcios de la industria u otros foros de normalización.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Véase norma.

Estándar abierto: Aquél que reúne las siguientes condiciones:

a) Que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

b) Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Herramientas genéricas: Instrumentos y programas de referencia, compartidos, de colaboración o componentes comunes y módulos similares reutilizables que satisfacen las necesidades comunes en los distintos ámbitos administrativos.

Imagen electrónica: Resultado de aplicar un proceso de digitalización a un documento.

Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus

actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Licencia Pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las 22 lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Lista de servicios de confianza (TSL): Lista de acceso público que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Modelo de datos: Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.

Nivel de resolución: Resolución espacial de la imagen obtenida como resultado de un proceso de digitalización.

Nodo de interoperabilidad: Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen.

Norma: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

a) norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público,

b) norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público,

c) norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La

política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

§ 28

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 4 de noviembre de 2015
Referencia: BOE-A-2010-1330

I

La necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En el ámbito de las Administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello ha venido a dar respuesta el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con sistemas de información del sector privado: empresas y administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse

efectivamente para evitar «tierras de nadie» y fracturas que pudieran dañar a la información o a los servicios prestados.

En este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

II

El Esquema Nacional de Seguridad tiene presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre Administración electrónica, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, Centro Criptológico Nacional, sociedad de la información, reutilización de la información en el sector público y órganos colegiados responsables de la Administración Electrónica; así como la regulación de diferentes instrumentos y servicios de la Administración, las directrices y guías de la OCDE y disposiciones nacionales e internacionales sobre normalización.

La Ley 11/2007, de 22 de junio, posibilita e inspira esta norma, a cuyo desarrollo coadyuva, en los aspectos de la seguridad de los sistemas de tecnologías de la información en las Administraciones públicas, contribuyendo al desarrollo de un instrumento efectivo que permite garantizar los derechos de los ciudadanos en la Administración electrónica.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal. Además, aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, referente legal imprescindible de cualquier regulación administrativa, determina la configuración de numerosos ámbitos de confidencialidad administrativos, diferentes a la información clasificada y a los datos de carácter personal, que necesitan ser materialmente protegidos. Asimismo determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones realizadas por vía electrónica.

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público que determina la regulación básica del régimen jurídico aplicable a la reutilización de documentos elaborados en el sector público, que configura un ámbito excepcionado de su aplicación, en el que se encuentra la información a la que se refiere el Esquema Nacional de Seguridad.

Junto a las disposiciones indicadas, han inspirado el contenido de esta norma, documentos de la Administración en materia de seguridad electrónica, tales como los Criterios de Seguridad, Normalización y Conservación, las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones, la Metodología y herramientas de análisis y gestión de riesgos o el Esquema Nacional de Interoperabilidad, también desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio.

III

Este real decreto se limita a establecer los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios, lo que exige incluir el alcance y procedimiento para gestionar la seguridad electrónica de los sistemas que tratan información

de las Administraciones públicas en el ámbito de la Ley 11/2007, de 22 de junio. Con ello, se logra un común denominador normativo, cuya regulación no agota todas las posibilidades de normación, y permite ser completada, mediante la regulación de los objetivos, materialmente no básicos, que podrán ser decididos por políticas legislativas territoriales.

Para dar cumplimiento a lo anterior se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad; se implanta la elaboración de un informe para conocer regularmente el estado de seguridad de los sistemas de información a los que se refiere el presente real decreto, se establece el papel de la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional, se incluye un glosario de términos y se hace una referencia expresa a la formación.

La norma se estructura en diez capítulos, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria y tres disposiciones finales. A los cuatro primeros anexos dedicados a la categoría de los sistemas, las medidas de seguridad, la auditoría de la seguridad, y el glosario de términos, se les une un quinto que establece un modelo de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes.

En este real decreto se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas. La información tratada en los sistemas electrónicos a los que se refiere este real decreto estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42 apartado 3 y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo, se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.

2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Artículo 2. *Definiciones y estándares.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de Términos incluido en el anexo IV.

Artículo 3. *Ámbito de aplicación.*

El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Artículo 5. *La seguridad como un proceso integral.*

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Artículo 6. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Artículo 7. *Prevención, reacción y recuperación.*

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 8. *Líneas de defensa.*

1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 9. *Reevaluación periódica.*

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Artículo 10. *La seguridad como función diferenciada.*

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Requisitos mínimos

Artículo 11. *Requisitos mínimos de seguridad.*

1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

2. A los efectos indicados en el apartado anterior, se considerarán órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los estatutos de autonomía correspondientes y normas de desarrollo; y la Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.

Los municipios podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan.

3. Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, y se cumplirán de acuerdo con lo establecido en el artículo 27.

Artículo 12. *Organización e implantación del proceso de seguridad.*

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

Artículo 13. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 14. *Gestión de personal.*

1. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

2. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

3. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

4. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Artículo 15. *Profesionalidad.*

1. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

2. El personal de las Administraciones públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

3. Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Artículo 16. *Autorización y control de los accesos.*

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Artículo 17. *Protección de las instalaciones.*

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

Artículo 18. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

4. Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en el artículo 15.

Artículo 19. *Seguridad por defecto.*

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Artículo 20. *Integridad y actualización del sistema.*

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Artículo 21. *Protección de información almacenada y en tránsito.*

1. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

3. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Artículo 22. *Prevención ante otros sistemas de información interconectados.*

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Artículo 23. *Registro de actividad.*

Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Artículo 24. *Incidentes de seguridad.*

1. Se establecerá un sistema de detección y reacción frente a código dañino.

2. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 25. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Artículo 26. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Artículo 27. *Cumplimiento de requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:

a) Los activos que constituyen el sistema.
b) La categoría del sistema, según lo previsto en el artículo 43.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

3. Los medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

4. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.

5. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad.

Artículo 28. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el presente real decreto en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.

Artículo 29. *Instrucciones técnicas de seguridad y guías de seguridad.*

1. Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.

2. El Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Para la redacción y mantenimiento de las

instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

3. Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas a nivel europeo que resulten de aplicación.

Artículo 30. *Sistemas de información no afectados.*

Las Administraciones públicas podrán determinar aquellos sistemas de información a los que no les sea de aplicación lo dispuesto en el presente de real decreto por tratarse de sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de junio.

CAPÍTULO IV

Comunicaciones electrónicas

Artículo 31. *Condiciones técnicas de seguridad de las comunicaciones electrónicas.*

1. Las condiciones técnicas de seguridad de las comunicaciones electrónicas en lo relativo a la constancia de la transmisión y recepción, de sus fechas, del contenido integro de las comunicaciones y la identificación fidedigna del remitente y destinatario de las mismas, según lo establecido en la Ley 11/2007, de 22 de junio, serán implementadas de acuerdo con lo establecido en el Esquema Nacional de Seguridad.

2. Las comunicaciones realizadas en los términos indicados en el apartado anterior, tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que resulte de aplicación.

Artículo 32. *Requerimientos técnicos de notificaciones y publicaciones electrónicas.*

1. Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el presente real decreto, las siguientes exigencias técnicas:

a) Aseguren la autenticidad del organismo que lo publique.

b) Aseguren la integridad de la información publicada.

c) Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.

d) Aseguren la autenticidad del destinatario de la publicación o notificación.

Artículo 33. *Firma electrónica.*

1. Los mecanismos de firma electrónica se aplicarán en los términos indicados en el Anexo II de esta norma y de acuerdo con lo preceptuado en la política de firma electrónica y de certificados, según se establece en el Esquema Nacional de Interoperabilidad.

2. La política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas, sin perjuicio de lo previsto en el Anexo II, que deberá adaptarse a cada circunstancia.

CAPÍTULO V

Auditoría de la seguridad

Artículo 34. *Auditoría de la seguridad.*

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

2. Esta auditoría se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.

3. En el marco de lo dispuesto en el artículo 39, de la ley 11/2007, de 22 de junio, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.

4. En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

5. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

6. Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

7. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

8. Los informes de auditoría podrán ser requeridos por los responsables de cada organización con competencias sobre seguridad de las tecnologías de la información.

CAPITULO VI

Estado de seguridad de los sistemas

Artículo 35. *Informe del estado de la seguridad.*

El Comité Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente Real Decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado.

CAPÍTULO VII

Respuesta a incidentes de seguridad

Artículo 36. *Capacidad de respuesta a incidentes de seguridad de la información.*

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y

de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del presente real decreto.

Artículo 37. *Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes de auditoría de los sistemas afectados, registros de auditoría, configuraciones y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y su normativa de desarrollo, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

c) Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquél, será coordinador a nivel público estatal.

CAPÍTULO VIII

Normas de conformidad

Artículo 38. *Sedes y registros electrónicos.*

La seguridad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Seguridad.

Artículo 39. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 40. *Mecanismos de control.*

Cada órgano de la Administración pública o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del Esquema Nacional de Seguridad.

Artículo 41. *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

CAPÍTULO IX

Actualización

Artículo 42. *Actualización permanente.*

El Esquema Nacional de Seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, de la evolución tecnológica y nuevos estándares internacionales sobre seguridad y auditoría en los sistemas y tecnologías de la información y a medida que vayan consolidándose las infraestructuras que le apoyan.

CAPÍTULO X

Categorización de los sistemas de información

Artículo 43. *Categorías.*

1. La categoría de un sistema de información, en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.
2. La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.
3. La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Artículo 44. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 43, así como la modificación posterior, en su caso, corresponderá, dentro del ámbito de su actividad, al responsable de cada información o servicio.
2. La facultad para determinar la categoría del sistema corresponderá al responsable del mismo.

Disposición adicional primera. *Formación.*

El personal de las Administraciones públicas recibirá, de acuerdo con lo previsto en la disposición adicional segunda de la Ley 11/2007, de 22 de junio, la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Seguridad, a cuyo fin los órganos responsables dispondrán lo necesario para que la formación sea una realidad efectiva.

Disposición adicional segunda. *Comité de Seguridad de la Información de las Administraciones Públicas.*

El Comité de Seguridad de la Información de las Administraciones Públicas, dependiente del Comité Sectorial de Administración electrónica, contará con un representante de cada una de las entidades presentes en dicho Comité Sectorial. Tendrá funciones de cooperación en materias comunes relacionadas con la adecuación e implantación de lo previsto en el Esquema Nacional de Seguridad y en las normas, instrucciones, guías y recomendaciones dictadas para su aplicación.

Disposición adicional tercera. *Modificación del Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.*

Se modifica la letra b) del apartado 5 del artículo 81 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal aprobado por Real Decreto 1720/2007, de 21 de diciembre, que pasa a tener la siguiente redacción:

«b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.»

Disposición adicional cuarta. *Desarrollo del Esquema Nacional de Seguridad.*

1. Sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica según lo establecido en el artículo 29, apartado 2, se desarrollarán las siguientes instrucciones técnicas de seguridad que serán de obligado cumplimiento por parte de las Administraciones públicas:

a) Informe del estado de la seguridad.
b) Notificación de incidentes de seguridad.
c) Auditoría de la seguridad.
d) Conformidad con el Esquema Nacional de Seguridad.
e) Adquisición de productos de seguridad.
f) Criptología de empleo en el Esquema Nacional de Seguridad.
g) Interconexión en el Esquema Nacional de Seguridad.
h) Requisitos de seguridad en entornos externalizados.

2. La aprobación de estas instrucciones se realizará de acuerdo con el procedimiento establecido en el citado artículo 29 apartados 2 y 3.

Disposición transitoria. *Adecuación de sistemas.*

1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXOS

ANEXO I

Categorías de los sistemas

1. Fundamentos para la determinación de la categoría de un sistema.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.

La determinación de la categoría de un sistema se realizará de acuerdo con lo establecido en el presente real decreto, y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general.

2. Dimensiones de la seguridad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

a) Disponibilidad [D].
b) Autenticidad [A].
c) Integridad [I].
d) Confidencialidad [C].
e) Trazabilidad [T].

3. Determinación del nivel requerido en una dimensión de seguridad.

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño menor por los activos de la organización.

3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.

5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1.º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño significativo por los activos de la organización.

3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.

5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3.º El incumplimiento grave de alguna ley o regulación.

4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5.º Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de un sistema de información.

1. Se definen tres categorías: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de un sistema sobre la base de lo indicado en el apartado anterior no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

5. Secuencia de actuaciones para determinar la categoría de un sistema:

1. Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3.

2. Determinación de la categoría del sistema, según lo establecido en el apartado 4.

ANEXO II

Medidas de seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.

b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría del sistema, según lo establecido en el Anexo I.
e) Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.
3. La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad del sistema.
4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad, es la que se indica en la tabla siguiente:

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento/Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local *(local logon)*
I C A T	aplica	+	=	op.acc.7	Acceso remoto *(remote login)*
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidentes
T	aplica	+	++	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidentes
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	aplica	=	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	**Medidas de protección**
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	aplica	+	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	aplica	=	=	mp.info.9	Copias de seguridad *(backup)*
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	+	mp.s.2	Protección de servicios y aplicaciones web

Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

En las tablas del presente Anexo se emplean las siguientes convenciones:

a) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad en algún nivel determinado se utiliza la voz «aplica».
b) «n.a.» significa «no aplica».
c) Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo «=».
d) Para indicar el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad, se utilizan los signos «+» y «++».
e) Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.
f) En las tablas del presente anexo se han empleado colores verde, amarillo y rojo de la siguiente forma: el color verde para indicar que una cierta medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar las medidas que empiezan a aplicarse en categoría MEDIA o superior; el rojo para indicar las medidas que sólo son de aplicación en categoría ALTA.

3. Marco organizativo [org]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.
b) El marco legal y regulatorio en el que se desarrollarán las actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que describan:

a) El uso correcto de equipos, servicios e instalaciones.
b) Lo que se considerará uso indebido.

c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que detallen de forma clara y precisa:

a) Cómo llevar a cabo las tareas habituales.
b) Quién debe hacer cada tarea.
c) Cómo identificar y reportar comportamientos anómalos.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:

a) Utilización de instalaciones, habituales y alternativas.
b) Entrada de equipos en producción, en particular, equipos que involucren criptografía.
c) Entrada de aplicaciones en producción.
d) Establecimiento de enlaces de comunicaciones con otros sistemas.
e) Utilización de medios de comunicación, habituales y alternativos.
f) Utilización de soportes de información.
g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.
h) Utilización de servicios de terceros, bajo contrato o Convenio.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:

a) Identifique los activos más valiosos del sistema.
b) Identifique las amenazas más probables.
c) Identifique las salvaguardas que protegen de dichas amenazas.
d) Identifique los principales riesgos residuales.

Categoría MEDIA

Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas más probables.
c) Identifique y valore las salvaguardas que protegen de dichas amenazas.
d) Identifique y valore el riesgo residual.

Categoría ALTA

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas posibles.
c) Identifique las vulnerabilidades habilitantes de dichas amenazas.
d) Identifique y valore las salvaguardas adecuadas.
e) Identifique y valore el riesgo residual.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	+

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

Categoría BÁSICA

a) Documentación de las instalaciones:

1. Áreas.
2. Puntos de acceso.

b) Documentación del sistema:

1. Equipos.
2. Redes internas y conexiones al exterior.
3. Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c) Esquema de líneas de defensa:

1. Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet o redes públicas en general.
2. Cortafuegos, DMZ, etc.
3. Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

d) Sistema de identificación y autenticación de usuarios:

1. Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
2. Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Categoría MEDIA

e) Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Categoría ALTA

f) Sistema de gestión de seguridad de la información con actualización y aprobación periódica.
g) Controles técnicos internos:

1. Validación de datos de entrada, salida y datos intermedios.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

a) Atenderá a las conclusiones del análisis de riesgos: [op.pl.1].
b) Será acorde a la arquitectura de seguridad escogida: [op.pl.2].
c) Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

4.1.4 Dimensionamiento / gestión de capacidades [op.pl.4].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

Con carácter previo a la puesta en explotación, se realizará un estudio previo que cubrirá los siguientes aspectos:

a) Necesidades de procesamiento.
b) Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
d) Necesidades de comunicación.
e) Necesidades de personal: cantidad y cualificación profesional.
f) Necesidades de instalaciones y medios auxiliares.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

Categoría ALTA

Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.
Una instrucción técnica de seguridad detallará los criterios exigibles.

4.2 Control de acceso. [op.acc].

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.
El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.
En todo control de acceso se requerirá lo siguiente:

a) Que todo acceso esté prohibido, salvo concesión expresa.
b) Que la entidad quede identificada singularmente [op.acc.1].
c) Que la utilización de los recursos esté protegida [op.acc.2].
d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].

f) Que la identidad de la entidad quede suficientemente autenticada [mp.acc.5].
g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.
2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.
3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:

a) Se puede saber quién recibe y qué derechos de acceso recibe.
b) Se puede saber quién ha hecho algo y qué ha hecho.

4. Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta estará asociada a un identificador único.
b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.
c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.

5. En los supuestos contemplados en el Capítulo IV relativo a "Comunicaciones Electrónicas", las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE:

– Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento n.º 910/2014)
– Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento n.º 910/2014)
– Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento n.º 910/2014).

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

Los requisitos de acceso se atenderán a lo que a continuación se indica:

a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	I C A T		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.
En concreto, se separarán al menos las siguientes funciones:

a) Desarrollo de operación.
b) Configuración y mantenimiento del sistema de operación.
c) Auditoría o supervisión de cualquier otra función.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada.
b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

4.2.5 Mecanismo de autenticación [op.acc.5].

dimensiones	ICAT		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

– "algo que se sabe": contraseñas o claves concertadas.

– "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, *tokens).*
– "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.
Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.
Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales.
Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:

– Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
– De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
– De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO

a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
c) Se atenderá a la seguridad de las credenciales de forma que:

1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) Se exigirá el uso de al menos dos factores de autenticación.
b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.
c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:

1. Presencial.
2. Telemático usando certificado electrónico cualificado.
3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO

a) Las credenciales se suspenderán tras un periodo definido de no utilización.
b) En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

4.2.6 Acceso local [op.acc.6].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización. Estos accesos tendrán en cuenta el nivel de las dimensiones de seguridad:

Nivel BAJO

a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso proporcionarán solamente la información indispensable).
b) El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.
c) Se registrarán los accesos con éxito, y los fallidos.
d) El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

Nivel MEDIO

Se informará al usuario del último acceso efectuado con su identidad.

Nivel ALTO

a) El acceso estará limitado por horario, fechas y lugar desde donde se accede.
b) Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

4.2.7 Acceso remoto [op.acc.7].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	=

Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.
Nivel BAJO
Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (como [op.acc.6]) como el canal de acceso remoto (como en [mp.com.2] y [mp.com.3]).

Nivel MEDIO

Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se configurarán los equipos previamente a su entrada en operación, de forma que:

a) Se retiren cuentas y contraseñas estándar.
b) Se aplicará la regla de «mínima funcionalidad»:

1.º El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,
2.º No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.
3.º Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.

c) Se aplicará la regla de «seguridad por defecto»:

1.º Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
2.º Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
3.º El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

4.3.3 Gestión de la configuración [op.exp.3].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

a) Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
b) Se mantenga en todo momento la regla de "seguridad por defecto" ([op.exp.2]).
c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).
d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).
e) El sistema reaccione a incidentes (ver [op.exp.7]).

4.3.4 Mantenimiento [op.exp.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.
b) Se efectuará un seguimiento continuo de los anuncios de defectos.
c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	todas		
categoría	básica	media	alta

	no aplica	aplica	=

Categoría MEDIA

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.
b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.
c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como «spyware», y en general, todo lo conocido como «malware».
Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

a) Procedimiento de reporte de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
d) Procedimientos para informar a las partes interesadas, internas y externas.
e) Procedimientos para:

1. Prevenir que se repita el incidente.
2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.

4.3.8 Registro de la actividad de los usuarios [op.exp.8].

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+	++

Se registrarán las actividades de los usuarios en el sistema, de forma que:

a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.
b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.
d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

Nivel BAJO

Se activarán los registros de actividad en los servidores.

Nivel MEDIO

Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO

Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
c) Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

4.3.10 Protección de los registros de actividad [op.exp.10].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se protegerán los registros del sistema, de forma que:

a) Se determinará el periodo de retención de los registros.
b) Se asegurará la fecha y hora. Ver [mp.info.5].
c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.
d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

4.3.11 Protección de claves criptográficas [op.exp.11].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	=

Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

Categoría BÁSICA

a) Los medios de generación estarán aislados de los medios de explotación.
b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Categoría MEDIA

a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5].
b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

4.4 Servicios externos [op.ext].

Cuando se utilicen recursos externos a la organización, sean servicios, equipos, instalaciones o personal, deberá tenerse en cuenta que la delegación se limita a las funciones.
La organización sigue siendo en todo momento responsable de los riesgos en que se incurre en la medida en que impacten sobre la información manejada y los servicios finales prestados por la organización.
La organización dispondrá las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.

4.4.2 Gestión diaria [op.ext.2].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Para la gestión diaria del sistema, se establecerán los siguientes puntos:

a) Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.

c) El mecanismo y los procedimientos de coordinación en caso de incidentes y desastres (ver [op.exp.7]).

4.4.3 Medios alternativos [op.ext.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo disfrutará de las mismas garantías de seguridad que el servicio habitual.

4.5 Continuidad del servicio [op.cont].

4.5.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

Se realizará un análisis de impacto que permita determinar:

a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
b) Los elementos que son críticos para la prestación de cada servicio.

4.5.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos:

a) Se identificarán funciones, responsabilidades y actividades a realizar.
b) Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.
c) Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
d) Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
e) El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

4.5.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad

4.6 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad.

4.6.1 Detección de intrusión [op.mon.1].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se dispondrán de herramientas de detección o de prevención de intrusión.

4.6.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA:

Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.

Categoría MEDIA:

Además, se recopilaran datos para valorar el sistema de gestión de incidentes, permitiendo conocer

– Número de incidentes de seguridad tratados.
– Tiempo empleado para cerrar el 50% de los incidentes.
– Tiempo empleado para cerrar el 90% de las incidentes.

Categoría ALTA

Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC:

– Recursos consumidos: horas y presupuesto.

5. Medidas de protección [mp]

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El equipamiento de instalará en áreas separadas específicas para su función.
Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	todas

categoría	básica	media	alta
	aplica	=	=

El mecanismo de control de acceso se atendrá a lo que se dispone a continuación:

a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.
b) Se registrarán las entradas y salidas de personas.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Los locales donde se ubiquen los sistemas de información y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial:

a) Condiciones de temperatura y humedad.
b) Protección frente a las amenazas identificadas en el análisis de riesgos.
c) Protección del cableado frente a incidentes fortuitos o deliberados.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+	=

Nivel BAJO

Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos:

a) Se garantizará el suministro de potencia eléctrica.
b) Se garantizará el correcto funcionamiento de las luces de emergencia.

Nivel MEDIO

Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	=	=

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento.

5.1.8 Instalaciones alternativas [mp.if.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles. Las instalaciones alternativas disfrutarán de las mismas garantías de seguridad que las instalaciones habituales.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Cada puesto de trabajo se caracterizará de la siguiente forma:

a) Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos.
b) Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.
c) Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

a) Se especificarán las medidas disciplinarias a que haya lugar.
b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.

2. En caso de personal contratado a través de un tercero:

a) Se establecerán los deberes y obligaciones del personal.
b) Se establecerán los deberes y obligaciones de cada parte.
c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.
En particular, se recordará regularmente:

a) La normativa de seguridad relativa al buen uso de los sistemas.
b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

5.2.4 Formación [mp.per.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción a incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

5.2.5 Personal alternativo [mp.per.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual. El personal alternativo deberá estar sometido a las mismas garantías de seguridad que el personal habitual.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	=

Categoría BÁSICA

Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento

Categoría MEDIA

Este material se guardará en lugar cerrado cuando no se esté utilizando.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	bajo	medio	alto
	no aplica	aplica	+

Nivel MEDIO

El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Nivel ALTO

Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

5.3.3 Protección de portátiles [mp.eq.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	+

Categoría BÁSICA

Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

a) Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

b) Se establecerá un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.

c) Cuando un equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de Internet y otras redes que no sean de confianza.

d) Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

Categoría ALTA

a) Se dotará al dispositivo de detectores de violación que permitan saber el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente.

b) La información de nivel alto almacenada en el disco se protegerá mediante cifrado.

5.3.4 Medios alternativos [mp.eq.9].

dimensiones	D		
nivel	bajo	medio	alto

	No aplica	aplica	=

Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.

Igualmente, se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	+

Categoría BÁSICA

Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.

Categoría ALTA

a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.

b) Se dispondrán sistemas redundantes.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	aplica	+

Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Nivel ALTO

a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

5.4.3 Protección de la autenticidad y de la integridad [mp.com.3].

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

Nivel BAJO

a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información (ver [op.acc.5]).

b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos:

1. La alteración de la información en tránsito.
2. La inyección de información espuria.
3. El secuestro de la sesión por una tercera parte.

c) Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación.

Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

Nivel ALTO

a) Se valorará positivamente el empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.
b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].
c) Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

5.4.4 Segregación de redes [mp.com.4].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.
Categoría ALTA
La red se segmentará en segmentos de forma que haya:

a) Control de entrada de los usuarios que llegan a cada segmento.
b) Control de salida de la información disponible en cada segmento.
c) Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado (como en [mp.com.1]).

5.4.5 Medios alternativos [mp.com.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de medios alternativos de comunicación para el caso de que fallen los medios habituales. Los medios alternativos de comunicación:

a) Estarán sujetos y proporcionar las mismas garantías de protección que el medio habitual.
b) Garantizarán un tiempo máximo de entrada en funcionamiento.

5.5 Protección de los soportes de información [mp.si].

5.5.1 Etiquetado [mp.si.1].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.

5.5.2 Criptografía [mp.si.2].

dimensiones	I C		
nivel	bajo	medio	alto
	no aplica	aplica	+

Esta medida se aplica, en particular, a todos los dispositivos removibles. Se entenderán por dispositivos removibles, los CD, DVD, discos USB, u otros de naturaleza análoga.

Nivel MEDIO

Se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

Nivel ALTO

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

5.5.3 Custodia [mp.si.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

a) Garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) ó lógicas ([mp.si.2]), o ambas.

b) Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

5.5.4 Transporte [mp.si.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

Para ello:

a) Se dispondrá de un registro de salida que identifique al transportista que recibe el soporte para su traslado.

b) Se dispondrá de un registro de entrada que identifique al transportista que lo entrega.

c) Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.

d) Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel.

e) Se gestionarán las claves según [op.exp.11].

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	D		
nivel	bajo	medio	alto

	no aplica	+	=

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1. Cuando la naturaleza del soporte no permita un borrado seguro.
2. Cuando así lo requiera el procedimiento asociado al tipo de información contenida.

c) Se emplearán productos certificados conforme a lo establecido en ([op. pl.5]).

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	bajo	medio	alto
	no aplica	aplica	=

Categoría MEDIA

a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.

b) Se aplicará una metodología de desarrollo reconocida que:

1.º Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
2.º Trate específicamente los datos usados en pruebas.
3.º Permita la inspección del código fuente.
4.º Incluya normas de programación segura.

c) Los siguientes elementos serán parte integral del diseño del sistema:

1.º Los mecanismos de identificación y autenticación.
2.º Los mecanismos de protección de la información tratada.
3.º La generación y tratamiento de pistas de auditoría.

d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

a) Se comprobará que:

1.º Se cumplen los criterios de aceptación en materia de seguridad.
2.º No se deteriora la seguridad de otros componentes del servicio.

b) Las pruebas se realizarán en un entorno aislado (pre-producción).

c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de vulnerabilidades.
b) Pruebas de penetración.

Categoría ALTA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de coherencia en la integración en los procesos.
b) Se considerará la oportunidad de realizar una auditoría de código fuente.

5.7 Protección de la información [mp.info].

5.7.1 Datos de carácter personal [mp.info.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.

Lo indicado en el párrafo anterior también se aplicará, cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	+	=

Nivel BAJO

1. Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma.
2. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
3. La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I.
4. El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
5. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Nivel MEDIO

Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.

f) Y cualquier otra actividad relacionada con dicha información.

5.7.3 Cifrado de la información [mp.info.3].

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Para el cifrado de información se estará a lo que se indica a continuación:

a) La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.
b) Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2].
c) Para el uso de criptografía en los soportes de información, se estará a lo dispuesto en [mp.si.2].

5.7.4 Firma electrónica [mp.info.4].

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.
La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.
En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del artículo 27.

Nivel BAJO

Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.
b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:
d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

1. Certificados.
2. Datos de verificación y validación.

e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d).
f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.

Nivel ALTO

1. Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma.
2. Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

5.7.5 Sellos de tiempo [mp.info.5].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Los sellos de tiempo prevendrán la posibilidad del repudio posterior:

1. Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
2. Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
3. Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.
4. Se utilizarán productos certificados (según [op.pl.5]) o servicios externos admitidos (véase [op.exp.10]).
5. Se emplearán "sellos cualificados de tiempo electrónicos" acordes con la normativa europea en la materia.

5.7.6 Limpieza de documentos [mp.info.6].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.
b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.
c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

5.7.7 Copias de seguridad (backup) [mp.info.9].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	=	=

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se

considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deberán abarcar:

g) Información de trabajo de la organización.

h) Aplicaciones en explotación, incluyendo los sistemas operativos.

i) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

j) Claves utilizadas para preservar la confidencialidad de la información.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico (e-mail) [mp.s.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.

b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1.º Correo no solicitado, en su expresión inglesa «spam».

2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.

3.º Código móvil de tipo «applet».

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1.º Limitaciones al uso como soporte de comunicaciones privadas.

2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
nivel	básica	media	alta
	aplica	=	+

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:

1.º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

2.º Se prevendrán ataques de manipulación de URL.

3.º Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies".

4.º Se prevendrán ataques de inyección de código.

b) Se prevendrán intentos de escalado de privilegios.

c) Se prevendrán ataques de "cross site scripting".

d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés".

Nivel BAJO

Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.

Nivel ALTO

Se emplearán "certificados cualificados de autenticación del sitio web" acordes a la normativa europea en la materia.

5.8.3 Protección frente a la denegación de servicio [mp.s.8].

dimensiones	D		
nivel	bajo	medio	alto
	No aplica	aplica	+

Nivel MEDIO

Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service). Para ello:

a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.
b) Se desplegarán tecnologías para prevenir los ataques conocidos.

Nivel ALTO

a) Se establecerá un sistema de detección de ataques de denegación de servicio.
b) Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.
c) Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

5.8.4 Medios alternativos [mp.s.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección que los medios habituales.

6. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

7. Interpretación

La interpretación del presente anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas CCN-STIC correspondientes a la implementación y a diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría.

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:

a) Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el artículo 18 «Adquisición de productos y contratación de servicios de seguridad».

2. Niveles de auditoría.

Los niveles de auditoría que se realizan a los sistemas de información, serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento del presente real decreto, identificará sus deficiencias y sugerirá las posibles medidas correctoras o complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.
b) Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación.

La interpretación del presente anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que

figura lo dispuesto en la instrucción técnica CCN-STIC correspondiente, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Categoría de un sistema. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Gestión de incidentes. Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Proceso. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Proceso de seguridad. Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.

Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Seguridad de las redes y de la información, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Servicios acreditados. Servicios prestados por un sistema con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación.

Sistema de gestión de la seguridad de la información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

Acrónimos

CCN: Centro Criptológico Nacional.

CERT: Computer Emergency Reaction Team.

INTECO: Instituto Nacional de Tecnologías de la Comunicación.

STIC: Seguridad de las Tecnologías de Información y Comunicaciones.

ANEXO V

Modelo de cláusula administrativa particular

Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 115.4 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, y en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre componentes certificados, recogida en el apartado 4.1.5 del anexo II del citado Real Decreto 3/2010, de 8 de enero.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

§ 29

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil

Jefatura del Estado
«BOE» núm. 15, de 17 de enero de 1996
Última modificación: 5 de junio de 2021
Referencia: BOE-A-1996-1069

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

EXPOSICIÓN DE MOTIVOS

1

La Constitución Española de 1978 al enumerar, en el capítulo III del Título I, los principios rectores de la política social y económica, hace mención en primer lugar a la obligación de los Poderes Públicos de asegurar la protección social, económica y jurídica de la familia y dentro de ésta, con carácter singular, la de los menores.

Esta preocupación por dotar al menor de un adecuado marco jurídico de protección trasciende también de diversos Tratados Internacionales ratificados en los últimos años por España y, muy especialmente, de la Convención de Derechos del Niño, de Naciones Unidas, de 20 de noviembre de 1989, ratificada por España el 30 de noviembre de 1990, que marca el inicio de una nueva filosofía en relación con el menor, basada en un mayor reconocimiento del papel que éste desempeña en la sociedad y en la exigencia de un mayor protagonismo para el mismo.

Esta necesidad ha sido compartida por otras instancias internacionales, como el Parlamento Europeo que, a través de la Resolución A 3-0172/92, aprobó la Carta Europea de los Derechos del Niño.

Consecuente con el mandato constitucional y con la tendencia general apuntada, se ha llevado a cabo, en los últimos años, un importante proceso de renovación de nuestro ordenamiento jurídico en materia de menores.

Primero fue la Ley 11/1981, de 13 de mayo, de modificación de la Filiación, Patria Potestad y Régimen Económico del Matrimonio, que suprimió la distinción entre filiación legítima e ilegítima, equiparó al padre y a la madre a efectos del ejercicio de la patria potestad e introdujo la investigación de la paternidad.

Después se han promulgado, entre otras, las Leyes 13/1983, de 24 de octubre, sobre la tutela; la Ley 21/1987, de 11 de noviembre, por la que se modifican determinados artículos del Código Civil y de la Ley de Enjuiciamiento Civil en materia de adopción; la Ley Orgánica 5/1988, de 9 de junio, sobre exhibicionismo y provocación sexual en relación con los menores; la Ley Orgánica 4/1992, de 5 de junio, sobre reforma de la Ley reguladora de la competencia y el procedimiento de los Juzgados de Menores; y la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, sobre la coordinación de disposiciones legales reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva.

De las Leyes citadas, la 21/1987, de 11 de noviembre, es la que, sin duda, ha introducido cambios más sustanciales en el ámbito de la protección del menor.

A raíz de la misma, el anticuado concepto de abandono fue sustituido por la institución del desamparo, cambio que ha dado lugar a una considerable agilización de los procedimientos de protección del menor al permitir la asunción automática, por parte de la entidad pública competente, de la tutela de aquél en los supuestos de desprotección grave del mismo.

Asimismo, introdujo la consideración de la adopción como un elemento de plena integración familiar, la configuración del acogimiento familiar como una nueva institución de protección del menor, la generalización del interés superior del menor como principio inspirador de todas las actuaciones relacionadas con aquél, tanto administrativas como judiciales; y el incremento de las facultades del Ministerio Fiscal en relación con los menores, así como de sus correlativas obligaciones.

No obstante, y pese al indudable avance que esta Ley supuso y a las importantes innovaciones que introdujo, su aplicación ha ido poniendo de manifiesto determinadas lagunas, a la vez que el tiempo transcurrido desde su promulgación ha hecho surgir nuevas necesidades y demandas en la sociedad.

Numerosas instituciones, tanto públicas como privadas -las dos Cámaras Parlamentarias, el Defensor del Pueblo, el Fiscal General del Estado y diversas asociaciones relacionadas con los menores-, se han hecho eco de estas demandas, trasladando al Gobierno la necesidad de adecuar el ordenamiento a la realidad de nuestra sociedad actual.

2

La presente Ley pretende ser la primera respuesta a estas demandas, abordando una reforma en profundidad de las tradicionales instituciones de protección del menor reguladas en el Código Civil.

En este sentido -y aunque el núcleo central de la Ley lo constituye, como no podía ser de otra forma, la modificación de los correspondientes preceptos del citado Código-, su contenido trasciende los límites de éste para construir un amplio marco jurídico de protección que vincula a todos los Poderes Públicos, a las instituciones específicamente relacionadas con los menores, a los padres y familiares y a los ciudadanos en general.

Las transformaciones sociales y culturales operadas en nuestra sociedad han provocado un cambio en el status social del niño y como consecuencia de ello se ha dado un nuevo enfoque a la construcción del edificio de los derechos humanos de la infancia.

Este enfoque reformula la estructura del derecho a la protección de la infancia vigente en España y en la mayoría de los países desarrollados desde finales del siglo XX, y consiste fundamentalmente en el reconocimiento pleno de la titularidad de derechos en los menores de edad y de una capacidad progresiva para ejercerlos.

El desarrollo legislativo postconstitucional refleja esta tendencia, introduciendo la condición de sujeto de derechos a las personas menores de edad. Así, el concepto «ser escuchado si tuviere suficiente juicio» se ha ido trasladando a todo el ordenamiento jurídico en todas aquellas cuestiones que le afectan. Este concepto introduce la dimensión del desarrollo evolutivo en el ejercicio directo de sus derechos.

Las limitaciones que pudieran derivarse del hecho evolutivo deben interpretarse de forma restrictiva. Más aún, esas limitaciones deben centrarse más en los procedimientos, de tal manera que se adoptarán aquéllos que sean más adecuados a la edad del sujeto.

El ordenamiento jurídico, y esta Ley en particular, va reflejando progresivamente una concepción de las personas menores de edad como sujetos activos, participativos y

creativos, con capacidad de modificar su propio medio personal y social; de participar en la búsqueda y satisfacción de sus necesidades y en la satisfacción de las necesidades de los demás.

El conocimiento científico actual nos permite concluir que no existe una diferencia tajante entre las necesidades de protección y las necesidades relacionadas con la autonomía del sujeto, sino que la mejor forma de garantizar social y jurídicamente la protección a la infancia es promover su autonomía como sujetos. De esta manera podrán ir construyendo progresivamente una percepción de control acerca de su situación personal y de su proyección de futuro. Este es el punto crítico de todos los sistemas de protección a la infancia en la actualidad. Y, por lo tanto, es el reto para todos los ordenamientos jurídicos y los dispositivos de promoción y protección de las personas menores de edad. Esta es la concepción del sujeto sobre la que descansa la presente Ley: las necesidades de los menores como eje de sus derechos y de su protección.

El Título I comienza enunciando un reconocimiento general de derechos contenidos en los Tratados Internacionales de los que España es parte, que además deben ser utilizados como mecanismo de interpretación de las distintas normas de aplicación a las personas menores de edad.

Por otra parte, del conjunto de derechos de los menores, se ha observado la necesidad de matizar algunos de ellos, combinando, por una parte, la posibilidad de su ejercicio con la necesaria protección que, por razón de la edad, los menores merecen.

Así, con el fin de reforzar los mecanismos de garantía previstos en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, se prohíbe la difusión de datos o imágenes referidos a menores de edad en los medios de comunicación cuando sea contrario a su interés, incluso cuando conste el consentimiento del menor. Con ello se pretende proteger al menor, que puede ser objeto de manipulación incluso por sus propios representantes legales o grupos en que se mueve. Completa esta modificación la legitimación activa al Ministerio Fiscal.

El derecho a la participación de los menores también se ha recogido expresamente en el articulado, con referencia al derecho a formar parte de asociaciones y a promover asociaciones infantiles y juveniles, con ciertos requisitos, que se completa con el derecho a participar en reuniones públicas y manifestaciones pacíficas, estableciéndose el requisito de la autorización de los padres, tutores o guardadores.

La Ley regula los principios generales de actuación frente a situaciones de desprotección social, incluyendo la obligación de la entidad pública de investigar los hechos que conozca para corregir la situación mediante la intervención de los Servicios Sociales o, en su caso, asumiendo la tutela del menor por ministerio de la ley.

De igual modo, se establece la obligación de toda persona que detecte una situación de riesgo o posible desamparo de un menor, de prestarle auxilio inmediato y de comunicar el hecho a la autoridad o sus agentes más próximos. Con carácter específico se prevé, asimismo, el deber de los ciudadanos de comunicar a las autoridades públicas competentes la ausencia del menor, de forma habitual o sin justificación, del centro escolar.

De innovadora se puede calificar la distinción, dentro de las situaciones de desprotección social del menor, entre situaciones de riesgo y de desamparo que dan lugar a un grado distinto de intervención de la entidad pública. Mientras en las situaciones de riesgo, caracterizadas por la existencia de un perjuicio para el menor que no alcanza la gravedad suficiente para justificar su separación del núcleo familiar, la citada intervención se limita a intentar eliminar, dentro de la institución familiar, los factores de riesgo, en las situaciones de desamparo, donde la gravedad de los hechos aconseja la extracción del menor de la familia, aquélla se concreta en la asunción por la entidad pública de la tutela del menor y la consiguiente suspensión de la patria potestad o tutela ordinaria.

Subyace a lo largo de la Ley una preocupación basada en la experiencia extraída de la aplicación de la Ley 21/1987, por agilizar y clarificar los trámites de los procedimientos administrativos y judiciales que afectan al menor, con la finalidad de que éste no quede indefenso o desprotegido en ningún momento.

Esta es la razón por la que, además de establecerse como principio general, el de que toda actuación habrá de tener fundamentalmente en cuenta el interés del menor y no interferir en su vida escolar, social o laboral, se determina que las resoluciones que aprecien

la existencia de la situación de desamparo deberán notificarse a los padres, tutores y guardadores, en un plazo de cuarenta y ocho horas, informándoles, asimismo, y, a ser posible, de forma presencial y de modo claro y comprensible, de las causas que dieron lugar a la intervención de la Administración y de los posibles efectos de la decisión adoptada.

Respecto a las medidas que los Jueces pueden adoptar para evitar situaciones perjudiciales para los hijos, que contempla actualmente el Código Civil en el artículo 158, se amplían a todos los menores, y a situaciones que exceden del ámbito de las relaciones paterno-filiales, haciéndose extensivas a las derivadas de la tutela y de la guarda, y se establece la posibilidad de que el Juez las adopte con carácter cautelar al inicio o en el curso de cualquier proceso civil o penal.

En definitiva, se trata de consagrar un principio de agilidad e inmediatez en todos los procedimientos tanto administrativos como judiciales que afectan a menores para evitar perjuicios innecesarios que puedan derivar de la rigidez de aquéllos.

Mención especial merece el acogimiento familiar, figura que introdujo la Ley 21/1987. Este puede constituirse por la entidad pública competente cuando concurre el consentimiento de los padres. En otro caso, debe dirigirse al Juez para que sea éste quien constituya el acogimiento. La aplicación de este precepto ha obligado, hasta ahora, a las entidades públicas a internar a los menores en algún centro, incluso en aquellos casos en los que la familia extensa ha manifestado su intención de acoger al menor, por no contar con la voluntad de los padres con el consiguiente perjuicio psicológico y emocional que ello lleva consigo para los niños, que se ven privados innecesariamente de la permanencia en un ambiente familiar.

Para remediar esta situación, la presente Ley recoge la posibilidad de que la entidad pública pueda acordar en interés del menor un acogimiento provisional en familia. Este podrá ser acordado por la entidad pública cuando los padres no consientan o se opongan al acogimiento, y subsistirá mientras se tramita el necesario expediente, en tanto no se produzca resolución judicial. De esta manera, se facilita la constitución del acogimiento de aquellos niños sobre los que sus padres han mostrado el máximo desinterés.

Hasta ahora, la legislación concebía el acogimiento como una situación temporal y por tanto la regulación del mismo no hacía distinciones respecto a las distintas circunstancias en que podía encontrarse el menor, dando siempre a la familia acogedora una autonomía limitada en cuanto al cuidado del menor.

Una reflexión que actualmente se está haciendo en muchos países es si las instituciones jurídicas de protección de menores dan respuesta a la diversidad de situaciones de desprotección en la que éstos se encuentran. La respuesta es que tanto la diversificación de instituciones jurídicas como la flexibilización de las prácticas profesionales, son indispensables para mejorar cualitativamente los sistemas de protección a la infancia. Esta Ley opta en esta dirección, flexibilizando la acogida familiar y adecuando el marco de relaciones entre los acogedores y el menor acogido en función de la estabilidad de la acogida.

Atendiendo a la finalidad del mismo, se recogen tres tipos de acogimiento. Junto al acogimiento simple, cuando se dan las condiciones de temporalidad, en las que es relativamente previsible el retorno del menor a su familia, se introduce la posibilidad de constituirlo con carácter permanente, en aquellos casos en los que la edad u otras circunstancias del menor o su familia aconsejan dotarlo de una mayor estabilidad, ampliando la autonomía de la familia acogedora respecto a las funciones derivadas del cuidado del menor, mediante la atribución por el Juez de aquellas facultades de la tutela que faciliten el desempeño de sus responsabilidades. También se recoge expresamente la modalidad del acogimiento preadoptivo que en la Ley 21/1987 aparecía únicamente en la exposición de motivos, y que también existe en otras legislaciones. Esta Ley prevé la posibilidad de establecer un período preadoptivo, a través de la formalización de un acogimiento con esta finalidad, bien sea porque la entidad pública eleve la propuesta de adopción de un menor o cuando considere necesario establecer un período de adaptación del menor a la familia antes de elevar al Juez dicha propuesta.

Con ello, se subsanan las insuficiencias de que adolecía el artículo 173.1 del Código Civil diferenciando entre los distintos tipos de acogimiento en función de que la situación de la familia pueda mejorar y que el retorno del menor no implique riesgos para éste, que las

circunstancias aconsejen que se constituya con carácter permanente, o que convenga constituirlo con carácter preadoptivo. También se contemplan los extremos que deben recogerse en el documento de formalización que el Código Civil exige.

En materia de adopción, la Ley introduce la exigencia del requisito de idoneidad de los adoptantes, que habrá de ser apreciado por la entidad pública, si es ésta la que formula la propuesta, o directamente por el Juez, en otro caso. Este requisito, si bien no estaba expresamente establecido en nuestro derecho positivo, su exigencia aparece explícitamente en la Convención de los Derechos del Niño y en el Convenio de La Haya sobre protección de menores y cooperación en materia de adopción internacional y se tenía en cuenta en la práctica en los procedimientos de selección de familias adoptantes.

La Ley aborda la regulación de la adopción internacional. En los últimos años se ha producido un aumento considerable de las adopciones de niños extranjeros por parte de adoptantes españoles. En el momento de la elaboración de la Ley 21/1987 no era un fenómeno tan extendido y no había suficiente perspectiva para abordarlo en dicha reforma. La Ley diferencia las funciones que han de ejercer directamente las entidades públicas de aquellas funciones de mediación que puedan delegar en agencias privadas que gocen de la correspondiente acreditación. Asimismo, establece las condiciones y requisitos para la acreditación de estas agencias, entre los que es de destacar la ausencia de fin de lucro por parte de las mismas.

Además se modifica el artículo 9.5 del Código Civil estableciendo la necesidad de la idoneidad de los adoptantes para la eficacia en nuestro país de las adopciones constituidas en el extranjero, dando de esta manera cumplimiento al compromiso adquirido en el momento de la ratificación de la Convención de Derechos del Niño de Naciones Unidas que obliga a los Estados Parte a velar porque los niños o niñas que sean adoptados en otro país gocen de los mismos derechos que los nacionales en la adopción.

Finalmente, se abordan también en la presente Ley algunos aspectos de la tutela, desarrollando aquellos artículos del Código Civil que requieren matizaciones cuando afecten a menores de edad. Así, la tutela de un menor de edad debe tender, cuando sea posible, a la integración del menor en la familia del tutor. Además se introduce como causa de remoción la existencia de graves y reiterados problemas de convivencia y se da en este procedimiento audiencia al menor.

En todo el texto aparece reforzada la intervención del Ministerio Fiscal, siguiendo la tendencia iniciada con la Ley 21/1987, ampliando los cauces de actuación de esta institución, a la que, por su propio Estatuto, corresponde la representación de los menores e incapaces que carezcan de representación legal.

Otra cuestión que se aborda en la Ley es el internamiento del menor en centro psiquiátrico y que con el objetivo de que se realice con las máximas garantías por tratarse de un menor de edad, se somete a la autorización judicial previa y a las reglas del artículo 211 del Código Civil, con informe preceptivo del Ministerio Fiscal, equiparando, a estos efectos, el menor al presunto incapaz y no considerando válido el consentimiento de sus padres para que el internamiento se considere voluntario, excepción hecha del internamiento de urgencia.

3

La Ley pretende ser respetuosa con el reparto constitucional y estatutario de competencias entre Estado y Comunidades Autónomas.

En este sentido, la Ley regula aspectos relativos a la legislación civil y procesal y a la Administración de Justicia, para los que goza de habilitación constitucional específica en los apartados 5.º, 6.º y 8.º del artículo 149.1.

No obstante, se dejan a salvo, en una disposición final específica, las competencias de las Comunidades Autónomas que dispongan de Derecho Civil, Foral o especial propio, para las que la Ley se declara subsidiaria respecto de las disposiciones específicas vigentes en aquéllas.

Asimismo, cuando se hace referencia a competencias de carácter administrativo, se especifica que las mismas corresponden a las Comunidades Autónomas y a las ciudades de Ceuta y Melilla, de conformidad con el reparto constitucional de competencias y las asumidas por aquéllas en sus respectivos Estatutos.

4

Por último se incorpora a la Ley la modificación de una serie de artículos del Código Civil con el fin de depurar los desajustes gramaticales y de contenido producidos por las sucesivas reformas parciales operadas en el Código.

Al margen de otras reformas que tan sólo afectaron tangencialmente a la institución de la tutela, la Ley 13/1983, de 24 de octubre, modificó el Título X del Libro I del Código Civil, rubricado «De la tutela, de la curatela y de la guarda de los menores o incapacitados» y mejoró el régimen de la tutela ordinaria que ya contemplaba el Código Civil. Asimismo, la Ley 21/1987, de 11 de noviembre, dio una nueva redacción a los artículos que regulan la tutela asumida por ministerio de la ley por las entidades públicas y cuya reforma ahora se aborda.

La coexistencia de estas dos vertientes de la institución de la tutela demanda una armonía interna en el Código Civil que la Sección Primera, de Derecho Privado, de la Comisión General de Codificación ha cubierto a través de la modificación de los artículos citados que, tras la reforma de 1983, ya resultaban incoherentes o de compleja aplicación práctica.

De este modo, y dado que la Ley tiene como objetivo básico la protección de los menores de edad a través de la tutela administrativa se ha incorporado la modificación de otros artículos en su gran mayoría conexos con esta materia.

TÍTULO I

De los derechos y deberes de los menores

CAPÍTULO I

Ámbito e interés superior del menor

Artículo 1. *Ambito de aplicación.*

La presente Ley y sus disposiciones de desarrollo son de aplicación a los menores de dieciocho años que se encuentren en territorio español, salvo que en virtud de la ley que les sea aplicable hayan alcanzado anteriormente la mayoría de edad.

Artículo 2. *Interés superior del menor.*

1. Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado. En la aplicación de la presente ley y demás normas que le afecten, así como en las medidas concernientes a los menores que adopten las instituciones, públicas o privadas, los Tribunales, o los órganos legislativos primará el interés superior de los mismos sobre cualquier otro interés legítimo que pudiera concurrir.

Las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva y, en todo caso, siempre en el interés superior del menor.

2. A efectos de la interpretación y aplicación en cada caso del interés superior del menor, se tendrán en cuenta los siguientes criterios generales, sin perjuicio de los establecidos en la legislación específica aplicable, así como de aquellos otros que puedan estimarse adecuados atendiendo a las circunstancias concretas del supuesto:

a) La protección del derecho a la vida, supervivencia y desarrollo del menor y la satisfacción de sus necesidades básicas, tanto materiales, físicas y educativas como emocionales y afectivas.

b) La consideración de los deseos, sentimientos y opiniones del menor, así como su derecho a participar progresivamente, en función de su edad, madurez, desarrollo y evolución personal, en el proceso de determinación de su interés superior.

c) La conveniencia de que su vida y desarrollo tenga lugar en un entorno familiar adecuado y libre de violencia. Se priorizará la permanencia en su familia de origen y se

preservará el mantenimiento de sus relaciones familiares, siempre que sea posible y positivo para el menor. En caso de acordarse una medida de protección, se priorizará el acogimiento familiar frente al residencial. Cuando el menor hubiera sido separado de su núcleo familiar, se valorarán las posibilidades y conveniencia de su retorno, teniendo en cuenta la evolución de la familia desde que se adoptó la medida protectora y primando siempre el interés y las necesidades del menor sobre las de la familia.

d) La preservación de la identidad, cultura, religión, convicciones, orientación e identidad sexual o idioma del menor, así como la no discriminación del mismo por éstas o cualesquiera otras condiciones, incluida la discapacidad, garantizando el desarrollo armónico de su personalidad.

3. Estos criterios se ponderarán teniendo en cuenta los siguientes elementos generales:

a) La edad y madurez del menor.

b) La necesidad de garantizar su igualdad y no discriminación por su especial vulnerabilidad, ya sea por la carencia de entorno familiar, sufrir maltrato, su discapacidad, su orientación e identidad sexual, su condición de refugiado, solicitante de asilo o protección subsidiaria, su pertenencia a una minoría étnica, o cualquier otra característica o circunstancia relevante.

c) El irreversible efecto del transcurso del tiempo en su desarrollo.

d) La necesidad de estabilidad de las soluciones que se adopten para promover la efectiva integración y desarrollo del menor en la sociedad, así como de minimizar los riesgos que cualquier cambio de situación material o emocional pueda ocasionar en su personalidad y desarrollo futuro.

e) La preparación del tránsito a la edad adulta e independiente, de acuerdo con sus capacidades y circunstancias personales.

f) Aquellos otros elementos de ponderación que, en el supuesto concreto, sean considerados pertinentes y respeten los derechos de los menores.

Los anteriores elementos deberán ser valorados conjuntamente, conforme a los principios de necesidad y proporcionalidad, de forma que la medida que se adopte en el interés superior del menor no restrinja o limite más derechos que los que ampara.

4. En caso de concurrir cualquier otro interés legítimo junto al interés superior del menor deberán priorizarse las medidas que, respondiendo a este interés, respeten también los otros intereses legítimos presentes.

En caso de que no puedan respetarse todos los intereses legítimos concurrentes, deberá primar el interés superior del menor sobre cualquier otro interés legítimo que pudiera concurrir.

Las decisiones y medidas adoptadas en interés superior del menor deberán valorar en todo caso los derechos fundamentales de otras personas que pudieran verse afectados.

5. Toda resolución de cualquier orden jurisdiccional y toda medida en el interés superior de la persona menor de edad deberá ser adoptada respetando las debidas garantías del proceso y, en particular:

a) Los derechos del menor a ser informado, oído y escuchado, y a participar en el proceso de acuerdo con la normativa vigente.

b) La intervención en el proceso de profesionales cualificados o expertos. En caso necesario, estos profesionales han de contar con la formación suficiente para determinar las específicas necesidades de los niños con discapacidad. En las decisiones especialmente relevantes que afecten al menor se contará con el informe colegiado de un grupo técnico y multidisciplinar especializado en los ámbitos adecuados.

c) La participación de progenitores, tutores o representantes legales del menor o de un defensor judicial si hubiera conflicto de interés o discrepancia con ellos y del Ministerio Fiscal en el proceso en defensa de sus intereses. Se presumirá que existe un conflicto de interés cuando la opinión de la persona menor de edad sea contraria a la medida que se adopte sobre ella o suponga una restricción de sus derechos.

d) La adopción de una decisión que incluya en su motivación los criterios utilizados, los elementos aplicados al ponderar los criterios entre sí y con otros intereses presentes y futuros, y las garantías procesales respetadas.

e) La existencia de recursos que permitan revisar la decisión adoptada que no haya considerado el interés superior del menor como primordial o en el caso en que el propio desarrollo del menor o cambios significativos en las circunstancias que motivaron dicha decisión hagan necesario revisarla. Los menores gozarán del derecho a la asistencia jurídica gratuita en los casos legalmente previstos.

CAPÍTULO II

Derechos del menor

Artículo 3. *Referencia a Instrumentos Internacionales.*

Los menores gozarán de los derechos que les reconoce la Constitución y los Tratados Internacionales de los que España sea parte, especialmente la Convención de Derechos del Niño de Naciones Unidas y la Convención de Derechos de las Personas con Discapacidad, y de los demás derechos garantizados en el ordenamiento jurídico, sin discriminación alguna por razón de nacimiento, nacionalidad, raza, sexo, discapacidad o enfermedad, religión, lengua, cultura, opinión o cualquier otra circunstancia personal, familiar o social.

La presente ley, sus normas de desarrollo y demás disposiciones legales relativas a las personas menores de edad, se interpretarán de conformidad con los Tratados Internacionales de los que España sea parte y, especialmente, de acuerdo con la Convención de los Derechos del Niño de Naciones Unidas y la Convención de Derechos de las Personas con Discapacidad.

Los poderes públicos garantizarán el respeto de los derechos de los menores y adecuarán sus actuaciones a la presente ley y a la mencionada normativa internacional.

Artículo 4. *Derecho al honor, a la intimidad y a la propia imagen.*

1. Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

2. La difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados.

3. Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

4. Sin perjuicio de las acciones de las que sean titulares los representantes legales del menor, corresponde en todo caso al Ministerio Fiscal su ejercicio, que podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública.

5. Los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros.

Artículo 5. *Derecho a la información.*

1. Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo. Se prestará especial atención a la alfabetización digital y mediática, de forma adaptada a cada etapa evolutiva, que permita a los menores actuar en línea con seguridad y responsabilidad y, en particular, identificar situaciones de riesgo derivadas de la utilización de las nuevas tecnologías de la información y la comunicación así como las herramientas y estrategias para afrontar dichos riesgos y protegerse de ellos.

2. Los padres o tutores y los poderes públicos velarán porque la información que reciban los menores sea veraz, plural y respetuosa con los principios constitucionales.

3. Las Administraciones Públicas incentivarán la producción y difusión de materiales informativos y otros destinados a los menores, que respeten los criterios enunciados, al mismo tiempo que facilitarán el acceso de los menores a los servicios de información, documentación, bibliotecas y demás servicios culturales incluyendo una adecuada sensibilización sobre la oferta legal de ocio y cultura en Internet y sobre la defensa de los derechos de propiedad intelectual.

En particular, velarán porque los medios de comunicación en sus mensajes dirigidos a menores promuevan los valores de igualdad, solidaridad, diversidad y respeto a los demás, eviten imágenes de violencia, explotación en las relaciones interpersonales, o que reflejen un trato degradante o sexista, o un trato discriminatorio hacia las personas con discapacidad. En el ámbito de la autorregulación, las autoridades y organismos competentes impulsarán entre los medios de comunicación, la generación y supervisión del cumplimiento de códigos de conducta destinados a salvaguardar la promoción de los valores anteriormente descritos, limitando el acceso a imágenes y contenidos digitales lesivos para los menores, a tenor de lo contemplado en los códigos de autorregulación de contenidos aprobados. Se garantizará la accesibilidad, con los ajustes razonables precisos, de dichos materiales y servicios, incluidos los de tipo tecnológico, para los menores con discapacidad.

Los poderes públicos y los prestadores fomentarán el disfrute pleno de la comunicación audiovisual para los menores con discapacidad y el uso de buenas prácticas que evite cualquier discriminación o repercusión negativa hacia dichas personas.

4. Para garantizar que la publicidad o mensajes dirigidos a menores o emitidos en la programación dirigida a éstos, no les perjudique moral o físicamente, podrá ser regulada por normas especiales.

5. Sin perjuicio de otros sujetos legitimados, corresponde en todo caso al Ministerio Fiscal y a las Administraciones públicas competentes en materia de protección de menores el ejercicio de las acciones de cese y rectificación de publicidad ilícita.

Artículo 6. *Libertad ideológica.*

1. El menor tiene derecho a la libertad de ideología, conciencia y religión.

2. El ejercicio de los derechos dimanantes de esta libertad tiene únicamente las limitaciones prescritas por la Ley y el respeto de los derechos y libertades fundamentales de los demás.

3. Los padres o tutores tienen el derecho y el deber de cooperar para que el menor ejerza esta libertad de modo que contribuya a su desarrollo integral.

Artículo 7. *Derecho de participación, asociación y reunión.*

1. Los menores tienen derecho a participar plenamente en la vida social, cultural, artística y recreativa de su entorno, así como a una incorporación progresiva a la ciudadanía activa.

Los poderes públicos promoverán la constitución de órganos de participación de los menores y de las organizaciones sociales de infancia y adolescencia.

Se garantizará la accesibilidad de los entornos y la provisión de ajustes razonables para que los menores con discapacidad puedan desarrollar su vida social, cultural, artística y recreativa.

2. Los menores tienen el derecho de asociación que, en especial, comprende:

a) El derecho a formar parte de asociaciones y organizaciones juveniles de los partidos políticos y sindicatos, de acuerdo con la Ley y los Estatutos.

b) El derecho a promover asociaciones infantiles y juveniles e inscribirlas de conformidad con la Ley. Los menores podrán formar parte de los órganos directivos de estas asociaciones.

Para que las asociaciones infantiles y juveniles puedan obligarse civilmente, deberán haber nombrado, de acuerdo con sus Estatutos, un representante legal con plena capacidad.

Cuando la pertenencia de un menor o de sus padres a una asociación impida o perjudique al desarrollo integral del menor, cualquier interesado, persona física o jurídica, o entidad pública, podrá dirigirse al Ministerio Fiscal para que promueva las medidas jurídicas de protección que estime necesarias.

3. Los menores tienen derecho a participar en reuniones públicas y manifestaciones pacíficas, convocadas en los términos establecidos por la Ley.

En iguales términos, tienen también derecho a promoverlas y convocarlas con el consentimiento expreso de sus padres, tutores o guardadores.

Artículo 8. *Derecho a la libertad de expresión.*

1. Los menores gozan del derecho a la libertad de expresión en los términos constitucionalmente previstos. Esta libertad de expresión tiene también su límite en la protección de la intimidad y la imagen del propio menor recogida en el artículo 4 de esta Ley.

2. En especial, el derecho a la libertad de expresión de los menores se extiende:

a) A la publicación y difusión de sus opiniones.
b) A la edición y producción de medios de difusión.
c) Al acceso a las ayudas que las Administraciones públicas establezcan con tal fin.

3. El ejercicio de este derecho podrá estar sujeto a las restricciones que prevea la Ley para garantizar el respeto de los derechos de los demás o la protección de la seguridad, salud, moral u orden público.

Artículo 9. *Derecho a ser oído y escuchado.*

1. El menor tiene derecho a ser oído y escuchado sin discriminación alguna por edad, discapacidad o cualquier otra circunstancia, tanto en el ámbito familiar como en cualquier procedimiento administrativo, judicial o de mediación en que esté afectado y que conduzca a una decisión que incida en su esfera personal, familiar o social, teniéndose debidamente en cuenta sus opiniones, en función de su edad y madurez. Para ello, el menor deberá recibir la información que le permita el ejercicio de este derecho en un lenguaje comprensible, en formatos accesibles y adaptados a sus circunstancias.

En los procedimientos judiciales o administrativos, las comparecencias o audiencias del menor tendrán carácter preferente, y se realizarán de forma adecuada a su situación y desarrollo evolutivo, con la asistencia, si fuera necesario, de profesionales cualificados o expertos, cuidando preservar su intimidad y utilizando un lenguaje que sea comprensible para él, en formatos accesibles y adaptados a sus circunstancias informándole tanto de lo que se le pregunta como de las consecuencias de su opinión, con pleno respeto a todas las garantías del procedimiento.

2. Se garantizará que el menor, cuando tenga suficiente madurez, pueda ejercitar este derecho por sí mismo o a través de la persona que designe para que le represente. La madurez habrá de valorarse por personal especializado, teniendo en cuenta tanto el desarrollo evolutivo del menor como su capacidad para comprender y evaluar el asunto concreto a tratar en cada caso. Se considera, en todo caso, que tiene suficiente madurez cuando tenga doce años cumplidos.

Para garantizar que el menor pueda ejercitar este derecho por sí mismo será asistido, en su caso, por intérpretes. El menor podrá expresar su opinión verbalmente o a través de formas no verbales de comunicación.

No obstante, cuando ello no sea posible o no convenga al interés del menor se podrá conocer la opinión del menor por medio de sus representantes legales, siempre que no tengan intereses contrapuestos a los suyos, o a través de otras personas que, por su profesión o relación de especial confianza con él, puedan transmitirla objetivamente.

3. Siempre que en vía administrativa o judicial se deniegue la comparecencia o audiencia de los menores directamente o por medio de persona que le represente, la resolución será motivada en el interés superior del menor y comunicada al Ministerio Fiscal, al menor y, en su caso, a su representante, indicando explícitamente los recursos existentes contra tal decisión. En las resoluciones sobre el fondo habrá de hacerse constar, en su caso, el resultado de la audiencia al menor, así como su valoración.

CAPÍTULO III

Deberes del menor

Artículo 9 bis. *Deberes de los menores.*

1. Los menores, de acuerdo a su edad y madurez, deberán asumir y cumplir los deberes, obligaciones y responsabilidades inherentes o consecuentes a la titularidad y al ejercicio de los derechos que tienen reconocidos en todos los ámbitos de la vida, tanto familiar, escolar como social.

2. Los poderes públicos promoverán la realización de acciones dirigidas a fomentar el conocimiento y cumplimiento de los deberes y responsabilidades de los menores en condiciones de igualdad, no discriminación y accesibilidad universal.

Artículo 9 ter. *Deberes relativos al ámbito familiar.*

1. Los menores deben participar en la vida familiar respetando a sus progenitores y hermanos así como a otros familiares.

2. Los menores deben participar y corresponsabilizarse en el cuidado del hogar y en la realización de las tareas domésticas de acuerdo con su edad, con su nivel de autonomía personal y capacidad, y con independencia de su sexo.

Artículo 9 quáter. *Deberes relativos al ámbito escolar.*

1. Los menores deben respetar las normas de convivencia de los centros educativos, estudiar durante las etapas de enseñanza obligatoria y tener una actitud positiva de aprendizaje durante todo el proceso formativo.

2. Los menores tienen que respetar a los profesores y otros empleados de los centros escolares, así como al resto de sus compañeros, evitando situaciones de conflicto y acoso escolar en cualquiera de sus formas, incluyendo el ciberacoso.

3. A través del sistema educativo se implantará el conocimiento que los menores deben tener de sus derechos y deberes como ciudadanos, incluyendo entre los mismos aquellos que se generen como consecuencia de la utilización en el entorno docente de las Tecnologías de la Información y Comunicación.

Artículo 9 quinquies. *Deberes relativos al ámbito social.*

1. Los menores deben respetar a las personas con las que se relacionan y al entorno en el que se desenvuelven.

2. Los deberes sociales incluyen, en particular:

a) Respetar la dignidad, integridad e intimidad de todas las personas con las que se relacionen con independencia de su edad, nacionalidad, origen racial o étnico, religión, sexo, orientación e identidad sexual, discapacidad, características físicas o sociales o pertenencia a determinados grupos sociales, o cualquier otra circunstancia personal o social.

b) Respetar las leyes y normas que les sean aplicables y los derechos y libertades fundamentales de las otras personas, así como asumir una actitud responsable y constructiva en la sociedad.

c) Conservar y hacer un buen uso de los recursos e instalaciones y equipamientos públicos o privados, mobiliario urbano y cualesquiera otros en los que desarrollen su actividad.

d) Respetar y conocer el medio ambiente y los animales, y colaborar en su conservación dentro de un desarrollo sostenible.

CAPÍTULO IV

Medidas y principios rectores de la acción administrativa

Artículo 10. *Medidas para facilitar el ejercicio de los derechos.*

1. Los menores tienen derecho a recibir de las Administraciones Públicas, o a través de sus entidades colaboradoras, la información en formato accesible y asistencia adecuada para el efectivo ejercicio de sus derechos, así como a que se garantice su respeto.

2. Para la defensa y garantía de sus derechos el menor puede:

a) Solicitar la protección y tutela de la entidad pública competente.

b) Poner en conocimiento del Ministerio Fiscal las situaciones que considere que atentan contra sus derechos con el fin de que éste promueva las acciones oportunas.

c) Plantear sus quejas ante el Defensor del Pueblo o ante las instituciones autonómicas homólogas. A tal fin, uno de los Adjuntos del Defensor del Pueblo se hará cargo de modo permanente de los asuntos relacionados con los menores facilitándoles el acceso a mecanismos adecuados y adaptados a sus necesidades y garantizándoles la confidencialidad.

d) Solicitar los recursos sociales disponibles de las Administraciones públicas.

e) Solicitar asistencia legal y el nombramiento de un defensor judicial, en su caso, para emprender las acciones judiciales y administrativas necesarias encaminadas a la protección y defensa de sus derechos e intereses. En todo caso el Ministerio Fiscal podrá actuar en defensa de los derechos de los menores.

f) Presentar denuncias individuales al Comité de Derechos del Niño, en los términos de la Convención sobre los Derechos del Niño y de la normativa que la desarrolle.

3. Los menores extranjeros que se encuentren en España tienen derecho a la educación, asistencia sanitaria y servicios y prestaciones sociales básicas, en las mismas condiciones que los menores españoles. Las Administraciones Públicas velarán por los grupos especialmente vulnerables como los menores extranjeros no acompañados, los que presenten necesidades de protección internacional, los menores con discapacidad y los que sean víctimas de abusos sexuales, explotación sexual, pornografía infantil, de trata o de tráfico de seres humanos, garantizando el cumplimiento de los derechos previstos en la ley.

Los poderes públicos, en el diseño y elaboración de las políticas públicas, tendrán como objetivo lograr la plena integración de los menores extranjeros en la sociedad española, mientras permanezcan en el territorio del Estado español, en los términos establecidos en la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.

4. Cuando la Entidad Pública asuma la tutela de un menor extranjero que se encuentre en España, la Administración General del Estado le facilitará, si no la tuviere, a la mayor celeridad, y junto con la presentación del certificado de tutela expedido por dicha Entidad Pública, la documentación acreditativa de su situación y la autorización de residencia, una vez que haya quedado acreditada la imposibilidad de retorno con su familia o al país de origen, y según lo dispuesto en la normativa vigente en materia de extranjería e inmigración.

5. Respecto de los menores tutelados o guardados por las Entidades Públicas, el reconocimiento de su condición de asegurado en relación con la asistencia sanitaria se realizará de oficio, previa presentación de la certificación de su tutela o guarda expedida por la Entidad Pública, durante el periodo de duración de las mismas.

Artículo 11. *Principios rectores de la acción administrativa.*

1. Las Administraciones Públicas facilitarán a los menores la asistencia adecuada para el ejercicio de sus derechos, incluyendo los recursos de apoyo que precisen.

Las Administraciones Públicas, en los ámbitos que les son propios, articularán políticas integrales encaminadas al desarrollo de la infancia y la adolescencia y, de modo especial, las referidas a los derechos enumerados en esta ley. Los menores tendrán derecho a acceder a tales servicios por sí mismos o a través de sus progenitores, tutores, guardadores o acogedores, quienes a su vez tendrán el deber de utilizarlos en interés de los menores.

Se impulsarán políticas compensatorias dirigidas a corregir las desigualdades sociales. En todo caso, el contenido esencial de los derechos del menor no podrá quedar afectado por falta de recursos sociales básicos. Se garantizará a los menores con discapacidad y a sus familias los servicios sociales especializados que su discapacidad precise.

Las Administraciones Públicas deberán tener en cuenta las necesidades de los menores al ejercer sus competencias, especialmente en materia de control sobre productos alimenticios, consumo, vivienda, educación, sanidad, servicios sociales, cultura, deporte, espectáculos, medios de comunicación, transportes, tiempo libre, juego, espacios libres y nuevas tecnologías (TICs).

Las Administraciones Públicas tendrán particularmente en consideración la adecuada regulación y supervisión de aquellos espacios, centros y servicios en los que permanezcan habitualmente menores, en lo que se refiere a sus condiciones físico-ambientales, higiénico-sanitarias, de accesibilidad y diseño universal y de recursos humanos, así como a sus proyectos educativos inclusivos, a la participación de los menores y a las demás condiciones que contribuyan a asegurar sus derechos.

2. Serán principios rectores de la actuación de los poderes públicos en relación con los menores:

a) La supremacía de su interés superior.

b) El mantenimiento en su familia de origen, salvo que no sea conveniente para su interés, en cuyo caso se garantizará la adopción de medidas de protección familiares y estables priorizando, en estos supuestos, el acogimiento familiar frente al institucional.

c) Su integración familiar y social.

d) La prevención y la detección precoz de todas aquellas situaciones que puedan perjudicar su desarrollo personal.

e) La sensibilización de la población ante situaciones de desprotección.

f) El carácter educativo de todas las medidas que se adopten.

g) La promoción de la participación, voluntariado y solidaridad social.

h) La objetividad, imparcialidad y seguridad jurídica en la actuación protectora, garantizando el carácter colegiado e interdisciplinar en la adopción de medidas que les afecten.

i) La protección contra toda forma de violencia, incluido el maltrato físico o psicológico, los castigos físicos humillantes y denigrantes, el descuido o trato negligente, la explotación, la realizada a través de las nuevas tecnologías, los abusos sexuales, la corrupción, la violencia de género o en el ámbito familiar, sanitario, social o educativo, incluyendo el acoso escolar, así como la trata y el tráfico de seres humanos, la mutilación genital femenina y cualquier otra forma de abuso.

j) La igualdad de oportunidades y no discriminación por cualquier circunstancia.

k) La accesibilidad universal de los menores con discapacidad y los ajustes razonables, así como su inclusión y participación plenas y efectivas.

l) El libre desarrollo de su personalidad conforme a su orientación e identidad sexual.

m) El respeto y la valoración de la diversidad étnica y cultural.

3. Los poderes públicos desarrollarán actuaciones encaminadas a la sensibilización, prevención, detección, notificación, asistencia y protección de cualquier forma de violencia contra la infancia y la adolescencia mediante procedimientos que aseguren la coordinación y la colaboración entre las distintas Administraciones, entidades colaboradoras y servicios competentes, tanto públicos como privados, para garantizar una actuación integral.

4. Las Entidades Públicas dispondrán de programas y recursos destinados al apoyo y orientación de quienes, estando en acogimiento, alcancen la mayoría de edad y queden fuera del sistema de protección, con especial atención a los que presentan discapacidad.

TÍTULO II

Actuaciones en situación de desprotección social del menor e instituciones de protección de menores

CAPÍTULO I

Actuaciones en situaciones de desprotección social del menor

Artículo 12. *Actuaciones de protección.*

1. La protección de los menores por los poderes públicos se realizará mediante la prevención, detección y reparación de situaciones de riesgo, con el establecimiento de los servicios y recursos adecuados para tal fin, el ejercicio de la guarda y, en los casos de declaración de desamparo, la asunción de la tutela por ministerio de la ley. En las actuaciones de protección deberán primar, en todo caso, las medidas familiares frente a las residenciales, las estables frente a las temporales y las consensuadas frente a las impuestas.

2. Los poderes públicos velarán para que los progenitores, tutores, guardadores o acogedores, desarrollen adecuadamente sus responsabilidades y les facilitarán servicios accesibles de prevención, asesoramiento y acompañamiento en todas las áreas que afectan al desarrollo de los menores.

3. Cuando los menores se encuentren bajo la patria potestad, tutela, guarda o acogimiento de una víctima de violencia de género o doméstica, las actuaciones de los poderes públicos estarán encaminadas a garantizar el apoyo necesario para procurar la permanencia de los menores, con independencia de su edad, con aquella, así como su protección, atención especializada y recuperación.

4. Cuando no pueda ser establecida la mayoría de edad de una persona, será considerada menor de edad a los efectos de lo previsto en esta ley, en tanto se determina su edad. A tal efecto, el Fiscal deberá realizar un juicio de proporcionalidad que pondere adecuadamente las razones por las que se considera que el pasaporte o documento equivalente de identidad presentado, en su caso, no es fiable. La realización de pruebas médicas para la determinación de la edad de los menores se someterá al principio de celeridad, exigirá el previo consentimiento informado del afectado y se llevará a cabo con respeto a su dignidad y sin que suponga un riesgo para su salud, no pudiendo aplicarse indiscriminadamente. No podrán realizarse, en ningún caso, desnudos integrales, exploraciones genitales u otras pruebas médicas especialmente invasivas.

Asimismo, una vez adoptada la medida de guarda o tutela respecto a personas menores de edad que hayan llegado solas a España, las Entidades Públicas comunicarán la adopción de dicha medida al Ministerio del Interior, a efectos de inscripción en el Registro Estatal correspondiente.

5. Las Entidades Públicas garantizarán los derechos reconocidos en esta ley a las personas menores de edad desde el momento que accede por primera vez a un recurso de protección y proporcionarán una atención inmediata integral y adecuada a sus necesidades, evitando la prolongación de las medidas de carácter provisional y de la estancia en los recursos de primera acogida.

6. Cualquier medida de protección no permanente que se adopte respecto de menores de tres años se revisará cada tres meses, y respecto de mayores de esa edad se revisará cada seis meses. En los acogimientos permanentes la revisión tendrá lugar el primer año cada seis meses y, a partir del segundo año, cada doce meses.

7. Además, de las distintas funciones atribuidas por ley, la Entidad Pública remitirá al Ministerio Fiscal informe justificativo de la situación de un determinado menor cuando este se haya encontrado en acogimiento residencial o acogimiento familiar temporal durante un periodo superior a dos años, debiendo justificar la Entidad Pública las causas por las que no se ha adoptado una medida protectora de carácter más estable en ese intervalo,

8. Los poderes públicos garantizarán los derechos y obligaciones de los menores con discapacidad en lo que respecta a su custodia, tutela, guarda, adopción o instituciones similares, velando al máximo por el interés superior del menor. Asimismo, garantizarán que los menores con discapacidad tengan los mismos derechos respecto a la vida en familia.

Para hacer efectivos estos derechos y a fin de prevenir su ocultación, abandono, negligencia o segregación velarán porque se proporcione con anticipación información, servicios y apoyo generales a los menores con discapacidad y a sus familias.

Artículo 13. *Obligaciones de los ciudadanos y deber de reserva.*

1. Toda persona o autoridad, especialmente aquellas que por su profesión, oficio o actividad detecten una situación de riesgo o posible desamparo de una persona menor de edad, lo comunicarán a la autoridad o sus agentes más próximos, sin perjuicio de prestarle el auxilio inmediato que precise.

2. Cualquier persona o autoridad que tenga conocimiento de que un menor no está escolarizado o no asiste al centro escolar de forma habitual y sin justificación, durante el período obligatorio, deberá ponerlo en conocimiento de las autoridades públicas competentes, que adoptarán las medidas necesarias para su escolarización.

3. Las autoridades y las personas que por su profesión o función conozcan el caso actuarán con la debida reserva.

En las actuaciones se evitará toda interferencia innecesaria en la vida del menor.

Artículo 14. *Atención inmediata.*

Las autoridades y servicios públicos tendrán la obligación de prestar la atención inmediata que precise cualquier menor, de actuar si corresponde a su ámbito de competencias o de dar traslado en otro caso al órgano competente y de poner los hechos en conocimiento de los representantes legales del menor o, cuando sea necesario, de la Entidad Pública y del Ministerio Fiscal.

La Entidad Pública podrá asumir, en cumplimiento de la obligación de prestar la atención inmediata, la guarda provisional de un menor prevista en el artículo 172.4 del Código Civil, que será comunicada al Ministerio Fiscal, procediendo simultáneamente a practicar las diligencias precisas para identificar al menor, investigar sus circunstancias y constatar, en su caso, la situación real de desamparo.

Artículo 14 bis. *Actuaciones en casos de urgencia.*

1. Cuando la urgencia del caso lo requiera, sin perjuicio de la guarda provisional a la que se refiere el artículo anterior y el artículo 172.4 del Código Civil, la actuación de los servicios sociales será inmediata.

2. La atención en casos de urgencia a que se refiere este artículo no está sujeta a requisitos procedimentales ni de forma, y se entiende en todo caso sin perjuicio del deber de prestar a las personas menores de edad el auxilio inmediato que precisen.

Artículo 15. *Principio de colaboración.*

En toda intervención se procurará contar con la colaboración del menor y su familia y no interferir en su vida escolar, social o laboral.

Artículo 16. *Evaluación de la situación.*

Las entidades públicas competentes en materia de protección de menores estarán obligadas a verificar la situación denunciada y a adoptar las medidas necesarias para resolverla en función del resultado de aquella actuación.

Artículo 17. *Actuaciones en situaciones de riesgo.*

1. Se considerará situación de riesgo aquella en la que, a causa de circunstancias, carencias o conflictos familiares, sociales o educativos, la persona menor de edad se vea perjudicada en su desarrollo personal, familiar, social o educativo, en su bienestar o en sus derechos de forma que, sin alcanzar la entidad, intensidad o persistencia que fundamentarían su declaración de situación de desamparo y la asunción de la tutela por ministerio de la ley, sea precisa la intervención de la administración pública competente, para eliminar, reducir o compensar las dificultades o inadaptación que le afectan y evitar su desamparo y exclusión social, sin tener que ser separado de su entorno familiar.

2. Serán considerados como indicadores de riesgo, entre otros:

a) La falta de atención física o psíquica del niño, niña o adolescente por parte de los progenitores, o por las personas que ejerzan la tutela, guarda, o acogimiento, que comporte un perjuicio leve para la salud física o emocional del niño, niña o adolescente cuando se estime, por la naturaleza o por la repetición de los episodios, la posibilidad de su persistencia o el agravamiento de sus efectos.

b) La negligencia en el cuidado de las personas menores de edad y la falta de seguimiento médico por parte de los progenitores, o por las personas que ejerzan la tutela, guarda o acogimiento.

c) La existencia de un hermano o hermana declarado en situación de riesgo o desamparo, salvo que las circunstancias familiares hayan cambiado de forma evidente.

d) La utilización, por parte de los progenitores, o de quienes ejerzan funciones de tutela, guarda o acogimiento, del castigo habitual y desproporcionado y de pautas de corrección violentas que, sin constituir un episodio severo o un patrón crónico de violencia, perjudiquen su desarrollo.

e) La evolución negativa de los programas de intervención seguidos con la familia y la obstrucción a su desarrollo o puesta en marcha.

f) Las prácticas discriminatorias, por parte de los responsables parentales, contra los niños, niñas y adolescentes que conlleven un perjuicio para su bienestar y su salud mental y física, en particular:

1.º Las actitudes discriminatorias que por razón de género, edad o discapacidad puedan aumentar las posibilidades de confinamiento en el hogar, la falta de acceso a la educación, las escasas oportunidades de ocio, la falta de acceso al arte y a la vida cultural, así como cualquier otra circunstancia que por razón de género, edad o discapacidad, les impidan disfrutar de sus derechos en igualdad.

2.º La no aceptación de la orientación sexual, identidad de género o las características sexuales de la persona menor de edad.

g) El riesgo de sufrir ablación, mutilación genital femenina o cualquier otra forma de violencia en el caso de niñas y adolescentes basadas en el género, las promesas o acuerdos de matrimonio forzado.

h) La identificación de las madres como víctimas de trata.

i) Las niñas y adolescentes víctimas de violencia de género en los términos establecidos en el artículo 1.1 de la Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género.

j) Los ingresos múltiples de personas menores de edad en distintos hospitales con síntomas recurrentes, inexplicables y/o que no se confirman diagnósticamente.

k) El consumo habitual de drogas tóxicas o bebidas alcohólicas por las personas menores de edad.

l) La exposición de la persona menor de edad a cualquier situación de violencia doméstica o de género.

m) Cualquier otra circunstancia que implique violencia sobre las personas menores de edad que, en caso de persistir, pueda evolucionar y derivar en el desamparo del niño, niña o adolescente.

3. La intervención en la situación de riesgo corresponde a la administración pública competente conforme a lo dispuesto en la legislación estatal y autonómica aplicable, en coordinación con los centros escolares y servicios sociales y sanitarios y, en su caso, con las entidades colaboradoras del respectivo ámbito territorial o cualesquiera otras.

4. La valoración de la situación de riesgo conllevará la elaboración y puesta en marcha de un proyecto de intervención social y educativo familiar que deberá recoger los objetivos, actuaciones, recursos y previsión de plazos, promoviendo los factores de protección del menor y manteniendo a éste en su medio familiar. Se procurará la participación de los progenitores, tutores, guardadores o acogedores en la elaboración del proyecto. En cualquier caso, será oída y tenida en cuenta la opinión de éstos en el intento de consensuar el proyecto, que deberá ser firmado por las partes, para lo que se les comunicará de manera

comprensible y en formato accesible. También se comunicará y consultará con el menor si tiene suficiente madurez y, en todo caso, a partir de los doce años.

5. Los progenitores, tutores, guardadores o acogedores, dentro de sus respectivas funciones, colaborarán activamente, según su capacidad, en la ejecución de las medidas indicadas en el referido proyecto. La omisión de la colaboración prevista en el mismo dará lugar a la declaración de la situación de riesgo del menor.

6. La situación de riesgo será declarada por la administración pública competente conforme a lo dispuesto en la legislación estatal y autonómica aplicable mediante una resolución administrativa motivada, previa audiencia a los progenitores, tutores, guardadores o acogedores y del menor si tiene suficiente madurez y, en todo caso, a partir de los doce años. La resolución administrativa incluirá las medidas tendentes a corregir la situación de riesgo del menor, incluidas las atinentes a los deberes al respecto de los progenitores, tutores, guardadores o acogedores. Frente a la resolución administrativa que declare la situación de riesgo del menor, se podrá interponer recurso conforme a la Ley de Enjuiciamiento Civil.

7. Cuando la administración pública competente esté desarrollando una intervención ante una situación de riesgo de un menor y tenga noticia de que va a ser trasladado al ámbito de otra entidad territorial, la administración pública de origen lo pondrá en conocimiento de la de destino al efecto de que, si procede, ésta continúe la intervención que se venía realizando, con remisión de la información y documentación necesaria. Si la administración pública de origen desconociera el lugar de destino, podrá solicitar el auxilio de las Fuerzas y Cuerpos de Seguridad a fin de que procedan a su averiguación. Una vez conocida la localización del menor, se pondrá en conocimiento de la Entidad Pública competente en dicho territorio, que continuará la intervención.

8. En los supuestos en que la administración pública competente para apreciar e intervenir en la situación de riesgo estime que existe una situación de desprotección que puede requerir la separación del menor de su ámbito familiar o cuando, concluido el período previsto en el proyecto de intervención o Convenio, no se hayan conseguido cambios en el desempeño de los deberes de guarda que garanticen que el menor cuenta con la necesaria asistencia moral o material, lo pondrá en conocimiento de la Entidad Pública a fin de que valore la procedencia de declarar la situación de desamparo, comunicándolo al Ministerio Fiscal.

Cuando la Entidad Pública considere que no procede declarar la situación de desamparo, pese a la propuesta en tal sentido formulada por la administración pública competente para apreciar la situación de riesgo, lo pondrá en conocimiento de la administración pública que haya intervenido en la situación de riesgo y del Ministerio Fiscal. Este último hará una supervisión de la situación del menor, pudiendo para ello recabar la colaboración de los centros escolares y los servicios sociales, sanitarios o cualesquiera otros.

9. La administración pública competente para intervenir en la situación de riesgo adoptará, en colaboración con los servicios de salud correspondientes, las medidas adecuadas de prevención, intervención y seguimiento, de las situaciones de posible riesgo prenatal, a los efectos de evitar con posterioridad una eventual declaración de situación de riesgo o desamparo del recién nacido. A tales efectos, se entenderá por situación de riesgo prenatal la falta de cuidado físico de la mujer gestante o el consumo abusivo de sustancias con potencial adictivo, así como cualquier otra acción propia de la mujer o de terceros tolerada por ésta, que perjudique el normal desarrollo o pueda provocar enfermedades o anomalías físicas, mentales o sensoriales al recién nacido. Los servicios de salud y el personal sanitario deberán notificar esta situación a la administración pública competente, así como al Ministerio Fiscal. Tras el nacimiento se mantendrá la intervención con el menor y su unidad familiar para que, si fuera necesario, se declare la situación de riesgo o desamparo del menor para su adecuada protección.

10. La negativa de los progenitores, tutores, guardadores o acogedores a prestar el consentimiento respecto de los tratamientos médicos necesarios para salvaguardar la vida o integridad física o psíquica de un menor constituye una situación de riesgo. En tales casos, las autoridades sanitarias, pondrán inmediatamente en conocimiento de la autoridad judicial,

directamente o a través del Ministerio Fiscal, tales situaciones a los efectos de que se adopte la decisión correspondiente en salvaguarda del mejor interés del menor.

Artículo 17 bis. *Personas menores de catorce años en conflicto con la ley.*

Las personas a las que se refiere el artículo 3 de la Ley Orgánica 5/2000, de 12 de enero, de responsabilidad penal de los menores serán incluidas en un plan de seguimiento que valore su situación socio-familiar diseñado y realizado por los servicios sociales competentes de cada comunidad autónoma.

Si el acto violento pudiera ser constitutivo de un delito contra la libertad o indemnidad sexual o de violencia de género, el plan de seguimiento deberá incluir un módulo formativo en igualdad de género.

Artículo 18. *Actuaciones en situación de desamparo.*

1. Cuando la Entidad Pública constate que el menor se encuentra en situación de desamparo, actuará en la forma prevista en el artículo 172 y siguientes del Código Civil, asumiendo la tutela de aquél por ministerio de la ley, adoptando las oportunas medidas de protección y poniéndolo en conocimiento del Ministerio Fiscal y, en su caso, del Juez que acordó la tutela ordinaria.

2. De acuerdo con lo establecido en el artículo 172 y siguientes del Código Civil, se considerará situación de desamparo la que se produce de hecho a causa del incumplimiento, o del imposible o inadecuado ejercicio de los deberes de protección establecidos por las leyes para la guarda de los menores, cuando éstos queden privados de la necesaria asistencia moral o material.

La situación de pobreza de los progenitores, tutores o guardadores no podrá ser tenida en cuenta para la valoración de la situación de desamparo. Asimismo, en ningún caso se separará a un menor de sus progenitores en razón de una discapacidad del menor, de ambos progenitores o de uno de ellos.

Se considerará un indicador de desamparo, entre otros, el tener un hermano declarado en tal situación, salvo que las circunstancias familiares hayan cambiado de forma evidente.

En particular se entenderá que existe situación de desamparo cuando se dé alguna o algunas de las siguientes circunstancias con la suficiente gravedad que, valoradas y ponderadas conforme a los principios de necesidad y proporcionalidad, supongan una amenaza para la integridad física o mental del menor:

a) El abandono del menor, bien porque falten las personas a las que por ley corresponde el ejercicio de la guarda, o bien porque éstas no quieran o no puedan ejercerla.

b) El transcurso del plazo de guarda voluntaria, bien cuando sus responsables legales se encuentren en condiciones de hacerse cargo de la guarda del menor y no quieran asumirla, o bien cuando, deseando asumirla, no estén en condiciones para hacerlo, salvo los casos excepcionales en los que la guarda voluntaria pueda ser prorrogada más allá del plazo de dos años.

c) El riesgo para la vida, salud e integridad física del menor. En particular cuando se produzcan malos tratos físicos graves, abusos sexuales o negligencia grave en el cumplimiento de las obligaciones alimentarias y de salud por parte de las personas de la unidad familiar o de terceros con consentimiento de aquellas; también cuando el menor sea identificado como víctima de trata de seres humanos y haya un conflicto de intereses con los progenitores, tutores y guardadores; o cuando exista un consumo reiterado de sustancias con potencial adictivo o la ejecución de otro tipo de conductas adictivas de manera reiterada por parte del menor con el conocimiento, consentimiento o la tolerancia de los progenitores, tutores o guardadores. Se entiende que existe tal consentimiento o tolerancia cuando no se hayan realizado los esfuerzos necesarios para paliar estas conductas, como la solicitud de asesoramiento o el no haber colaborado suficientemente con el tratamiento, una vez conocidas las mismas. También se entiende que existe desamparo cuando se produzcan perjuicios graves al recién nacido causados por maltrato prenatal.

d) El riesgo para la salud mental del menor, su integridad moral y el desarrollo de su personalidad debido al maltrato psicológico continuado o a la falta de atención grave y crónica de sus necesidades afectivas o educativas por parte de progenitores, tutores o guardadores. Cuando esta falta de atención esté condicionada por un trastorno mental

grave, por un consumo habitual de sustancias con potencial adictivo o por otras conductas adictivas habituales, se valorará como un indicador de desamparo la ausencia de tratamiento por parte de progenitores, tutores o guardadores o la falta de colaboración suficiente durante el mismo.

e) El incumplimiento o el imposible o inadecuado ejercicio de los deberes de guarda como consecuencia del grave deterioro del entorno o de las condiciones de vida familiares, cuando den lugar a circunstancias o comportamientos que perjudiquen el desarrollo del menor o su salud mental.

f) La inducción a la mendicidad, delincuencia o prostitución, o cualquier otra explotación del menor de similar naturaleza o gravedad.

g) La ausencia de escolarización o falta de asistencia reiterada y no justificada adecuadamente al centro educativo y la permisividad continuada o la inducción al absentismo escolar durante las etapas de escolarización obligatoria.

h) Cualquier otra situación gravemente perjudicial para el menor que traiga causa del incumplimiento o del imposible o inadecuado ejercicio de la patria potestad, la tutela o la guarda, cuyas consecuencias no puedan ser evitadas mientras permanezca en su entorno de convivencia.

3. Cada Entidad Pública designará al órgano que ejercerá la tutela de acuerdo con sus estructuras orgánicas de funcionamiento.

4. En caso de traslado permanente de residencia de un menor sujeto a una medida de protección desde la Comunidad Autónoma que la adoptó a otra distinta, corresponde a ésta asumir aquella medida o adoptar la que proceda en un plazo máximo de tres meses desde que esta última sea informada por la primera de dicho traslado. No obstante lo anterior, cuando la familia de origen del menor permanezca en la Comunidad Autónoma de origen y sea previsible una reintegración familiar a corto o medio plazo, se mantendrá la medida adoptada y la Entidad Pública del lugar de residencia del menor colaborará en el seguimiento de la evolución de éste. Tampoco será necesaria la adopción de nuevas medidas de protección en los casos de traslado temporal de un menor a un centro residencial ubicado en otra Comunidad Autónoma o cuando se establezca un acogimiento con familia residente en ella, con el acuerdo de ambas Comunidades Autónomas.

5. En los supuestos en los que se detecte una situación de posible desprotección de un menor de nacionalidad española que se encuentre fuera del territorio nacional, para su protección en España será competente la Entidad Pública correspondiente a la Comunidad Autónoma en la que residan los progenitores o tutores del menor. En su defecto, será competente la Entidad Pública correspondiente a la Comunidad Autónoma con la cual el menor o sus familiares tuvieren mayores vínculos. Cuando, conforme a tales criterios, no pudiere determinarse la competencia, será competente la Entidad Pública de la Comunidad Autónoma en la que el menor o sus familiares hubieran tenido su última residencia habitual.

En todo caso, cuando el menor que se encuentra fuera de España hubiera sido objeto de una medida de protección previamente a su desplazamiento, será competente la Entidad Pública que ostente su guarda o tutela.

Los posibles conflictos de competencia que pudieran originarse habrán de resolverse conforme a los principios de celeridad y de interés superior del menor, evitando dilaciones en la toma de decisiones que pudieran generar perjuicios al mismo.

La Administración General del Estado se encargará del traslado del menor a España. La Comunidad Autónoma que corresponda asumirá la competencia desde el momento en que el menor se encuentre en España.

6. En los supuestos en que las medidas de protección adoptadas en un Estado extranjero deban cumplirse en España, se atenderá, en primer lugar, a lo previsto en el Reglamento (CE) n.º 2201/2003 del Consejo, de 27 de noviembre de 2003, relativo a la competencia, el reconocimiento y la ejecución de las resoluciones judiciales en materia matrimonial y de responsabilidad parental, por el que se deroga el Reglamento (CE) n.º 1347/2000, o norma europea que lo sustituya. En los casos no regulados por la normativa europea, se estará a los Tratados y Convenios internacionales en vigor para España y, en especial, al Convenio relativo a la competencia, la ley aplicable, el reconocimiento, la ejecución y la cooperación en materia de responsabilidad parental y de medidas de protección de los niños, hecho en La Haya el 19 de octubre de 1996, o Convenio que lo

sustituya. En defecto de toda normativa internacional, se estará a las normas españolas de producción interna sobre eficacia en España de medidas de protección de menores.

Artículo 19. *Guarda de menores.*

1. Además de la guarda de los menores tutelados por encontrarse en situación de desamparo, la Entidad Pública deberá asumir la guarda en los términos previstos en el artículo 172 bis del Código Civil, cuando los progenitores o tutores no puedan cuidar de un menor por circunstancias graves y transitorias o cuando así lo acuerde el Juez en los casos en que legalmente proceda.

2. La guarda voluntaria tendrá una duración máxima de dos años, salvo que el interés superior del menor aconseje, excepcionalmente, la prórroga de la medida por la previsible reintegración familiar en un plazo breve de tiempo.

En estos supuestos de guarda voluntaria será necesario el compromiso de la familia de someterse, en su caso, a la intervención profesional.

Artículo 19 bis. *Disposiciones comunes a la guarda y tutela.*

1. Cuando la Entidad Pública asuma la tutela o guarda del menor elaborará un plan individualizado de protección que establecerá los objetivos, la previsión y el plazo de las medidas de intervención a adoptar con su familia de origen, incluido, en su caso, el programa de reintegración familiar.

En el caso de tratarse de un menor con discapacidad, la Entidad Pública garantizará la continuidad de los apoyos que viniera recibiendo o la adopción de otros más adecuados para sus necesidades.

2. Cuando del pronóstico se derive la posibilidad de retorno a la familia de origen, la Entidad Pública aplicará el programa de reintegración familiar, todo ello sin perjuicio de lo dispuesto en la normativa relativa a los menores extranjeros no acompañados.

3. Para acordar el retorno del menor desamparado a su familia de origen será imprescindible que se haya comprobado una evolución positiva de la misma, objetivamente suficiente para restablecer la convivencia familiar, que se hayan mantenido los vínculos, que concurra el propósito de desempeñar las responsabilidades parentales adecuadamente y que se constate que el retorno con ella no supone riesgos relevantes para el menor a través del correspondiente informe técnico. En los casos de acogimiento familiar, deberá ponderarse, en la toma de decisión sobre el retorno, el tiempo transcurrido y la integración en la familia de acogida y su entorno, así como el desarrollo de vínculos afectivos con la misma.

4. Cuando se proceda a la reunificación familiar, la Entidad Pública realizará un seguimiento posterior de apoyo a la familia del menor.

5. En el caso de los menores extranjeros no acompañados, se procurará la búsqueda de su familia y el restablecimiento de la convivencia familiar, iniciando el procedimiento correspondiente, siempre que se estime que dicha medida responde a su interés superior y no coloque al menor o a su familia en una situación que ponga en riesgo su seguridad.

6. Las menores y las jóvenes sujetas a medidas de protección que estén embarazadas, recibirán el asesoramiento y el apoyo adecuados a su situación. En el plan individual de protección se contemplará esta circunstancia, así como la protección del recién nacido.

Artículo 20. *Acogimiento familiar.*

1. Cuando no sea posible la permanencia en el entorno familiar de origen, el acogimiento familiar, de acuerdo con su finalidad y con independencia del procedimiento en que se acuerde, revestirá las modalidades establecidas en el Código Civil y, en razón de la vinculación del menor con la familia acogedora, podrá tener lugar, de acuerdo al interés superior del menor, en la propia familia extensa del menor o en familia ajena.

El acogimiento familiar podrá ser especializado, entendiendo por tal el que se desarrolla en una familia en la que alguna o algunas de las personas que integran la unidad familiar dispone de cualificación, experiencia o formación específica para desempeñar esta función respecto de menores con necesidades o circunstancias especiales, pudiendo percibir por ello una compensación.

El acogimiento especializado podrá ser de dedicación exclusiva cuando así se determine por la Entidad Pública por razón de las necesidades y circunstancias especiales del menor en situación de ser acogido, percibiendo en tal caso la persona o personas designadas como acogedoras una compensación en atención a dicha dedicación.

2. El acogimiento familiar se formalizará por resolución de la Entidad Pública que tenga la tutela o la guarda, previa valoración de la adecuación de la familia para el acogimiento. En esta valoración se tendrá en cuenta su situación familiar y aptitud educadora, su capacidad para atender adecuadamente las necesidades de toda índole del menor o menores de que se trate, la congruencia entre su motivación y la naturaleza y finalidad del acogimiento según su modalidad, así como la disposición a facilitar el cumplimiento de los objetivos del plan individual de atención y, si lo hubiera, del programa de reintegración familiar, propiciando la relación del menor con su familia de procedencia. El régimen de visitas podrá tener lugar en los puntos de encuentro familiar habilitados, cuando así lo aconseje el interés superior del menor y el derecho a la privacidad de las familias de procedencia y acogedora. Cuando el tipo de acogimiento así lo aconseje, se valorará la adecuación de la edad de los acogedores con la del menor acogido, así como la relación previa entre ellos, priorizando, salvo que el interés del menor aconseje otra cosa, a las personas que, perteneciendo a su familia extensa, reúnan condiciones adecuadas para el acogimiento.

3. A la resolución de formalización del acogimiento familiar a que se refiere el apartado anterior, acordada conforme a los términos previstos en el Código Civil, se acompañará un documento anexo que incluirá los siguientes extremos:

a) La identidad del acogedor o acogedores y del acogido.

b) Los consentimientos y audiencias necesarias.

c) La modalidad del acogimiento, duración prevista para el mismo, así como su carácter de acogimiento en familia extensa o en familia ajena en razón de la vinculación del menor con la familia o persona acogedora.

d) Los derechos y deberes de cada una de las partes, y en particular:

1.º El régimen de visitas, estancia, relación o comunicación, en los supuestos de declaración de desamparo, por parte de la familia de origen, que podrá modificarse por la Entidad Pública en atención al interés superior del menor.

2.º El sistema de cobertura por parte de la Entidad Pública de los daños que sufra el menor o de los que pueda causar a terceros.

3.º La asunción por parte de los acogedores de los gastos de manutención, educación y atención socio-sanitaria.

e) El contenido del seguimiento que, en función de la finalidad del acogimiento, vaya a realizar la Entidad Pública y el compromiso de colaboración con dicho seguimiento por parte de la familia acogedora.

f) En el caso de menores con discapacidad, los recursos de apoyo que precisa.

g) La compensación económica, apoyos técnicos y otro tipo de ayudas que, en su caso, vayan a recibir los acogedores.

h) El plazo en el cual la medida vaya a ser revisada.

La resolución y el documento anexo se remitirán al Ministerio Fiscal en el plazo máximo de un mes.

Artículo 20 bis. *Derechos y deberes de los acogedores familiares.*

1. Los acogedores familiares tendrán derecho a:

a) Recibir información acerca de la naturaleza y efectos del acogimiento, así como preparación previa, seguimiento y apoyo técnico especializado durante y al término del mismo. En el caso de menores con discapacidad, los acogedores tendrán derecho a orientación, acompañamiento y apoyo adaptados a la discapacidad del menor.

b) Ser oídos por la Entidad Pública antes de que ésta adopte cualquier resolución que afecte al menor, especialmente antes de modificar o suspender temporalmente el régimen de visitas o de relación o comunicación con la familia de origen.

c) Ser informados del plan individual de protección así como de las medidas de protección relacionadas con el acogimiento que se adopten respecto al menor acogido, de

las revisiones periódicas y a obtener información del expediente de protección del menor que les resulte necesaria para el ejercicio de sus funciones, a excepción de aquellas cuestiones relacionadas con el derecho a la intimidad de terceros y a la protección de datos de carácter personal.

d) Ser parte en todos los procesos de oposición a las medidas de protección y a la declaración de situación de desamparo del menor acogido y en todos los procesos de oposición relacionados con la medida de acogimiento familiar permanente con funciones de tutela que tenga formalizada.

e) Cooperar con la Entidad Pública en los planes de actuación y seguimiento establecidos para el acogimiento.

f) Disponer de la documentación identificativa, sanitaria y educativa del menor que acogen.

g) Ejercer todos los derechos inherentes a la guarda.

h) Ser respetados por el menor acogido.

i) Recabar el auxilio de la Entidad Pública en el ejercicio de sus funciones.

j) Realizar viajes con el menor siempre que se informe a la Entidad Pública y no exista oposición de ésta.

k) Percibir una compensación económica y otro tipo de ayuda que se hubiera estipulado, en su caso.

l) Facilitar al menor acogido las mismas condiciones que a los hijos biológicos o adoptados, a fin de hacer uso de derechos u obligaciones familiares durante el tiempo que el menor conviva con ellos.

m) Relacionarse con el menor al cesar el acogimiento, si la Entidad Pública entiende que conviniere a su interés superior y lo consintieren la familia de origen o, en su caso, la familia adoptiva o de acogimiento permanente, y el menor si tuviere suficiente madurez y, en todo caso, si fuera mayor de doce años.

n) Ser protegidos sus datos personales respecto de la familia de origen, de acuerdo con la legislación vigente.

ñ) Formular formalmente quejas o sugerencias ante la Entidad Pública que deberán ser tramitadas en un plazo inferior a los 30 días y, en caso de solicitar audiencia, ser escuchado con anterioridad a dicho plazo.

o) La familia acogedora tendrá los mismos derechos que la Administración reconoce al resto de unidades familiares.

2. Los acogedores familiares tendrán los siguientes deberes:

a) Velar por el bienestar y el interés superior del menor, tenerlo en su compañía, alimentarlo, educarlo y procurarle una formación integral en un entorno afectivo. En el caso de menor con discapacidad, deberá continuar prestando los apoyos especializados que viniera recibiendo o adoptar otros más adecuados a sus necesidades.

b) Oír al menor siempre antes de tomar decisiones que le afecten, si tuviere suficiente madurez y, en todo caso, si fuera mayor de 12 años, sin exclusión alguna por discapacidad, y a transmitir a la Entidad Pública las peticiones que éste pueda realizar dentro de su madurez.

c) Asegurar la plena participación del menor en la vida de familia.

d) Informar a la Entidad Pública de cualquier hecho de trascendencia en relación con el menor.

e) Respetar y facilitar las relaciones con la familia de origen del menor, en la medida de las posibilidades de los acogedores familiares, en el marco del régimen de visitas establecido a favor de aquella y la reintegración familiar, en su caso.

f) Colaborar activamente con las Entidades Públicas en el desarrollo de la intervención individualizada con el menor y seguimiento de la medida, observando las indicaciones y orientaciones de la misma.

g) Respetar la confidencialidad de los datos relativos a los antecedentes personales y familiares del menor.

h) Comunicar a la Entidad Publica cualquier cambio en la situación familiar relativo a los datos y circunstancias que se tomaron en consideración como base para el acogimiento.

i) Garantizar el derecho a la intimidad y a la identidad de los menores acogidos y el respeto a su propia imagen, así como velar por el cumplimiento de sus derechos fundamentales.

j) Participar en las acciones formativas que se propongan.

k) Colaborar en el tránsito de la medida de protección del menor a la reintegración a su entorno de origen, la adopción, u otra modalidad de acogimiento, o al entorno que se establezca tras la adopción de una medida de protección más estable.

l) Los acogedores familiares tendrán las mismas obligaciones respecto del menor acogido que aquellos que la ley establece para los titulares de la patria potestad.

Artículo 20 ter. *Tramitación de las solicitudes de acogimiento transfronterizo de personas menores de edad en España remitidas por un Estado miembro de la Unión Europea o por un Estado parte del Convenio de La Haya de 1996.*

1. El Ministerio de Justicia, en su calidad de Autoridad Central Española, será la autoridad competente para recibir las solicitudes de acogimiento transfronterizo de personas menores de edad procedentes de un Estado miembro de la Unión Europea o de un Estado parte del Convenio de La Haya de 1996. Dichas solicitudes deberán ser remitidas por la Autoridad Central del Estado requirente al objeto de obtener la preceptiva autorización de las autoridades españolas competentes con carácter previo a que se pueda producir el acogimiento.

2. Las solicitudes de acogimiento deberán realizarse por escrito y acompañarse de los documentos que la Autoridad Central española requiera para valorar la idoneidad de la medida en beneficio de la persona menor de edad y la aptitud del establecimiento o familia para llevar a cabo dicho acogimiento. En todo caso, además de la requerida por la normativa internacional aplicable, deberá aportarse un informe sobre el niño, niña o adolescente, los motivos de su propuesta de acogimiento, la modalidad de acogimiento, la duración del mismo y cómo se prevé hacer seguimiento de la medida.

3. Recibida la solicitud de acogimiento transfronterizo, la Autoridad Central española comprobará que la solicitud reúne el contenido y los requisitos según lo previsto en el apartado anterior y la transmitirá a la Administración autonómica competente para su aprobación.

4. La Administración autonómica competente, una vez evaluada la solicitud, remitirá su decisión a la Autoridad Central española que la hará llegar a la Autoridad Central del Estado requirente. Únicamente en caso de ser favorable, las autoridades competentes de dicho Estado dictarán una resolución que ordene el acogimiento en España, notificarán a todas las partes interesadas y solicitarán su reconocimiento y ejecución en España directamente ante el Juzgado o Tribunal español territorialmente competente.

5. El plazo máximo para la tramitación y respuesta de la solicitud será de tres meses.

6. Las solicitudes de acogimiento y sus documentos adjuntos deberán acompañarse de una traducción legalizada en español.

Artículo 20 quater. *Motivos de denegación de las solicitudes de acogimiento transfronterizo de personas menores de edad en España.*

1. La Autoridad Central española rechazará las solicitudes de acogimiento transfronterizo cuando:

a) El objeto o finalidad de la solicitud de acogimiento no garantice el interés superior de la persona menor de edad para lo cual se tendrá especialmente en cuenta la existencia de vínculos con España.

b) La solicitud no reúna los requisitos exigidos para su tramitación. En este caso, se devolverá a la Autoridad Central requirente indicando los motivos concretos de la devolución con el fin de que pueda subsanarlos.

c) Se solicite el desplazamiento de una persona menor de edad incursa en un procedimiento penal o sancionador o que haya sido condenada o sancionada por la comisión de cualquier ilícito penal o administrativo.

d) No se haya respetado el derecho fundamental de la persona menor de edad a ser oída y escuchada, así como a mantener contactos con sus progenitores o representantes legales, salvo si ello es contrario a su superior interés.

Artículo 20 quinquies. *Del procedimiento para la transmisión de las solicitudes de acogimiento transfronterizo de personas menores de edad desde España a otro Estado miembro de la Unión Europea o a un Estado parte del Convenio de La Haya de 1996.*

1. Las solicitudes de acogimiento transfronterizo que soliciten las Autoridades competentes en materia de protección de personas menores de edad se remitirán por escrito a la Autoridad Central española, que las transmitirá a las autoridades competentes del Estado miembro requerido para su tramitación.
2. La tramitación y aprobación de dichas solicitudes se regirá por el Derecho Nacional del Estado miembro requerido.
3. La Autoridad Central española remitirá la decisión del acogimiento requerido a la Autoridad solicitante.
4. Las solicitudes de acogimiento y los documentos adjuntos que se dirijan a una autoridad extranjera deberán acompañarse de una traducción a una lengua oficial del Estado requerido o aceptada por este.

Artículo 21. *Acogimiento residencial.*

1. En relación con los menores en acogimiento residencial, las Entidades Públicas y los servicios y centros donde se encuentren deberán actuar conforme a los principios rectores de esta ley, con pleno respeto a los derechos de los menores acogidos, y tendrán las siguientes obligaciones básicas:

a) Asegurarán la cobertura de las necesidades de la vida cotidiana y garantizarán los derechos de los menores adaptando su proyecto general a las características personales de cada menor, mediante un proyecto socio-educativo individual, que persiga el bienestar del menor, su desarrollo físico, psicológico, social y educativo en el marco del plan individualizado de protección que defina la Entidad Pública.
b) Contarán con el plan individual de protección de cada menor que establezca claramente la finalidad del ingreso, los objetivos a conseguir y el plazo para su consecución, en el cual se preverá la preparación del menor, tanto a la llegada como a la salida del centro.
c) Adoptarán todas sus decisiones en relación con el acogimiento residencial de los menores en interés de los mismos.
d) Fomentarán la convivencia y la relación entre hermanos siempre que ello redunde en interés de los menores y procurarán la estabilidad residencial de los menores, así como que el acogimiento tenga lugar preferentemente en un centro ubicado en la provincia de origen del menor.
e) Promoverán la relación y colaboración familiar, programándose, al efecto, los recursos necesarios para posibilitar el retorno a su familia de origen, si se considera que ese es el interés del menor.
f) Potenciarán la educación integral e inclusiva de los menores, con especial consideración a las necesidades de los menores con discapacidad, y velarán por su preparación para la vida plena, de manera especial su escolarización y formación.
En el caso de los menores de dieciséis a dieciocho años uno de los objetivos prioritarios será la preparación para la vida independiente, la orientación e inserción laboral.
g) Poseerán una normativa interna de funcionamiento y convivencia que responda a las necesidades educativas y de protección, y tendrán recogido un procedimiento de formulación de quejas y reclamaciones.
h) Administrarán los medicamentos que, en su caso, precisen los menores bajo prescripción y seguimiento médico, de acuerdo con la praxis profesional sanitaria. A estos efectos se llevará un registro con la historia médica de cada uno de los menores.
i) Revisarán periódicamente el plan individual de protección con el objeto de valorar la adecuación del recurso residencial a las circunstancias personales del menor.

j) Potenciarán las salidas de los menores en fines de semana y períodos vacacionales con sus familias de origen o, cuando ello no fuese posible o procedente, con familias alternativas.

k) Promoverán la integración normalizada de los menores en los servicios y actividades de ocio, culturales y educativas que transcurran en el entorno comunitario en el que se encuentran.

l) Establecerán los necesarios mecanismos de coordinación con los servicios sociales especializados para el seguimiento y ajuste de las medidas de protección.

m) Velarán por la preparación para la vida independiente, promoviendo la participación en las decisiones que le afecten, incluida la propia gestión del centro, la autonomía y la asunción progresiva de responsabilidades.

n) Establecerán medidas educativas y de supervisión que garanticen la protección de los datos personales del menor al acceder a las tecnologías de la información y de la comunicación y a las redes sociales.

2. Todos los centros de acogimiento residencial que presten servicios dirigidos a menores en el ámbito de la protección deberán estar siempre habilitados administrativamente por la Entidad Pública, debiendo respetar el régimen de habilitación lo dispuesto en la Ley 20/2013, de 9 de diciembre, de garantía de la unidad de mercado. Además, deberán existir estándares de calidad y accesibilidad por cada tipo de servicio.

La Entidad Pública regulará el régimen de funcionamiento de los centros de acogimiento residencial e inscribirá en el registro correspondiente a las entidades de acuerdo con sus disposiciones, prestando especial atención a la seguridad, sanidad, accesibilidad para personas con discapacidad, número, ratio y cualificación profesional de su personal, proyecto educativo, participación de los menores en su funcionamiento interno y demás condiciones que contribuyan a asegurar sus derechos.

Asimismo, la Entidad Pública promoverá modelos de acogimiento residencial con núcleos reducidos de menores que convivan en condiciones similares a las familiares.

3. Con el fin de favorecer que la vida del menor se desarrolle en un entorno familiar, prevalecerá la medida de acogimiento familiar sobre la de acogimiento residencial para cualquier menor, especialmente para menores de seis años. No se acordará el acogimiento residencial para menores de tres años salvo en supuestos de imposibilidad, debidamente acreditada, de adoptar en ese momento la medida de acogimiento familiar o cuando esta medida no convenga al interés superior del menor. Esta limitación para acordar el acogimiento residencial se aplicará también a los menores de seis años en el plazo más breve posible. En todo caso, y con carácter general, el acogimiento residencial de estos menores no tendrá una duración superior a tres meses.

4. A los efectos de asegurar la protección de los derechos de los menores, la Entidad Pública deberá realizar la inspección y supervisión de los centros y servicios semestralmente y siempre que así lo exijan las circunstancias.

5. Asimismo, el Ministerio Fiscal deberá ejercer la vigilancia sobre las decisiones de acogimiento residencial que se adopten, así como la inspección sobre todos los servicios y centros de acogimiento residencial, analizando, entre otros, los Proyectos Educativos Individualizados, el Proyecto Educativo del Centro y el Reglamento Interno.

6. La administración pública competente podrá adoptar las medidas adecuadas para garantizar la convivencia del centro, actuando sobre aquellas conductas con medidas de carácter educativo, que no podrán atentar, en ningún caso, contra la dignidad de los menores. En casos graves de perturbación de la convivencia, podrán limitarse las salidas del centro de acogida. Estas medidas deberán ejercerse de forma inmediata y proporcional a la conducta de los menores, teniendo en cuenta las circunstancias personales de éstos, su actitud y los resultados derivados de su comportamiento.

7. De aquellas medidas que se impusieran por conductas o actitudes que fueren atentatorias contra la convivencia en el ámbito residencial, se dará cuenta inmediata a los progenitores, tutores o representantes legales del menor y al Ministerio Fiscal.

Artículo 21 bis. *Derechos de los menores acogidos.*

1. El menor acogido, con independencia de la modalidad de acogimiento en que se encuentre, tendrá derecho a:

a) Ser oído en los términos del artículo 9 y, en su caso, ser parte en el proceso de oposición a las medidas de protección y declaración en situación de desamparo de acuerdo con la normativa aplicable, y en función de su edad y madurez. Para ello tiene derecho a ser informado y notificado de todas las resoluciones de formalización y cese del acogimiento.

b) Ser reconocido beneficiario del derecho de asistencia jurídica gratuita cuando se encuentre en situación de desamparo.

c) Dirigirse directamente a la Entidad Pública y ser informado de cualquier hecho trascendente relativo al acogimiento.

d) Relacionarse con su familia de origen en el marco del régimen de visitas, relación y comunicación establecido por la Entidad Pública.

e) Conocer progresivamente su realidad socio-familiar y sus circunstancias para facilitar la asunción de las mismas.

f) Recibir con la suficiente anticipación la información, los servicios y los apoyos generales que sean necesarios para hacer efectivos los derechos de los menores con discapacidad.

g) Poner en conocimiento del Ministerio Fiscal las reclamaciones o quejas que considere, sobre las circunstancias de su acogimiento.

h) Recibir el apoyo educativo y psicoterapéutico por parte de la Entidad Pública, para superar trastornos psicosociales de origen, medida esta aplicable tanto en acogimiento residencial, como en acogimiento familiar.

i) Recibir el apoyo educativo y psicoterapéutico que sea necesario.

j) Acceder a su expediente y conocer los datos sobre sus orígenes y parientes biológicos, una vez alcanzada la mayoría de edad.

2. En los supuestos de acogimiento familiar, tiene, además, los siguientes derechos:

a) Participar plenamente en la vida familiar del acogedor.

b) Mantener relación con la familia de acogida tras el cese del acogimiento si la Entidad Pública entiende que conviniere a su interés superior y siempre que lo consintieren el menor si tuviere suficiente madurez y, en todo caso, si fuera mayor de doce años, la familia de acogida y la de origen o, en su caso, la familia adoptiva o de acogimiento permanente.

c) Solicitar información o pedir, por sí mismo si tuviera suficiente madurez, el cese del acogimiento familiar.

3. En los supuestos de acogimiento residencial, tiene, además, los siguientes derechos:

a) Respeto a la privacidad y a conservar sus pertenencias personales siempre que no sean inadecuadas para el contexto educativo.

b) Participar en la elaboración de la programación de actividades del centro y en el desarrollo de las mismas.

c) Ser escuchado en caso de queja y ser informado de todos los sistemas de atención y reclamación que tienen a su alcance, incluido el derecho de audiencia en la Entidad Pública.

Artículo 21 ter. *Medidas para garantizar la convivencia y la seguridad en los centros de protección a la infancia y la adolescencia.*

1. Las medidas adoptadas para garantizar la convivencia y la seguridad en los centros de protección a la infancia y la adolescencia, consistirán en medidas de carácter preventivo y de desescalada, pudiéndose también adoptar excepcionalmente y como último recurso, medidas de contención física del menor.

Se prohíbe la contención mecánica, consistente en la sujeción de una persona menor de edad o a una cama articulada o a un objeto fijo o anclado a las instalaciones o a objetos muebles.

2. Toda medida que se aplique en un centro de protección a la infancia y la adolescencia para garantizar la convivencia y seguridad se regirá por los principios de legalidad,

necesidad, individualización, proporcionalidad, idoneidad, graduación, transparencia y buen gobierno.

Asimismo, la ejecución de las medidas de contención se regirá por los principios rectores de excepcionalidad, mínima intensidad posible y tiempo estrictamente necesario, y se llevarán a cabo con el respeto debido a la dignidad, a la privacidad y a los derechos de la persona menor de edad.

3. Las medidas de desescalada y de contención deberán aplicarse por personal especializado con formación en materia de derechos de la infancia y la adolescencia, así como en resolución de conflictos y técnicas de sujeción personal.

4. Las medidas de desescalada consistirán en todas aquellas técnicas verbales de gestión emocional conducentes a la reducción de la tensión u hostilidad del menor que se encuentre en estado de alteración y/o agitación con inminente y grave peligro para su vida e integridad o para la de otras personas.

5. Las medidas de contención física podrán consistir en la interposición entre el menor y la persona u objeto que se encuentra en peligro, la restricción física de espacios o movimientos y, en última instancia, bajo un estricto protocolo, la inmovilización física del menor por personal especializado del centro.

Como medida excepcional y únicamente aplicable en centros de protección de menores con trastornos de conducta, la medida de contención física podrá consistir en la sujeción de las muñecas del menor con equipos homologados, que se aplicará con las garantías previstas en el artículo 28 de esta ley.

6. Las medidas de contención aplicadas en los centros de protección a la infancia y la adolescencia deberán ser comunicadas con carácter inmediato a la Entidad Pública y al Ministerio Fiscal. Asimismo, se anotarán en el Libro Registro de Incidencias, que será supervisado por parte de la dirección del centro y en el expediente individualizado del menor, que debe mantenerse actualizado.

La aplicación de medidas de contención requerirá, en todos los casos en que se hiciera uso de la fuerza, la exploración física del menor por facultativo médico en el plazo máximo de 48 horas, extendiéndose el correspondiente parte médico.

7. Las medidas de contención no podrán aplicarse a personas menores de catorce años, a las menores gestantes, a las menores hasta seis meses después de la terminación del embarazo, a las madres lactantes, a las personas que tengan hijos e hijas consigo, ni a quienes se encuentren convalecientes por enfermedad grave, salvo que de la actuación de aquellos pudiera derivarse un inminente y grave peligro para su vida e integridad o para la de otras personas.

Corresponde al Director del Centro o persona en la que este haya delegado, la adopción de decisiones sobre las medidas de contención física consistentes en la restricción de espacios y movimientos o la inmovilización del menor, que deberán ser motivadas y habrán de notificarse con carácter inmediato a la Entidad Pública y al Ministerio Fiscal.

Artículo 22. *Información a los familiares.*

La entidad pública que tenga menores bajo su guarda o tutela deberá informar a los padres, tutores o guardadores sobre la situación de aquéllos cuando no exista resolución judicial que lo prohíba.

Artículo 22 bis. *Programas de preparación para la vida independiente.*

Las Entidades Públicas ofrecerán programas de preparación para la vida independiente dirigidos a los jóvenes que estén bajo una medida de protección, particularmente en acogimiento residencial o en situación de especial vulnerabilidad, desde dos años antes de su mayoría de edad, una vez cumplida esta, siempre que lo necesiten, con el compromiso de participación activa y aprovechamiento por parte de los mismos. Los programas deberán propiciar seguimiento socioeducativo, alojamiento, inserción socio-laboral, apoyo psicológico y ayudas económicas.

Artículo 22 ter. *Sistema de información sobre la protección a la infancia y a la adolescencia.*

Las Comunidades Autónomas y la Administración General del Estado establecerán un sistema de información compartido que permita el conocimiento uniforme de la situación de la protección a la infancia y a la adolescencia en España, y de ofrecimientos para el acogimiento y la adopción, con datos desagregados por género y discapacidad, tanto a efectos de seguimiento de las medidas concretas de protección de menores como a efectos estadísticos. A estos mismos efectos se desarrollará el Registro Unificado de Maltrato Infantil.

Artículo 22 quáter. *Tratamiento de datos de carácter personal.*

1. Para el cumplimiento de las finalidades previstas en el capítulo I del título II de esta ley, las Administraciones Públicas competentes podrán proceder, sin el consentimiento del interesado, a la recogida y tratamiento de los datos que resulten necesarios para valorar la situación del menor, incluyendo tanto los relativos al mismo como los relacionados con su entorno familiar o social.

Los profesionales, las Entidades Públicas y privadas y, en general, cualquier persona facilitarán a las Administraciones Públicas los informes y antecedentes sobre los menores, sus progenitores, tutores, guardadores o acogedores, que les sean requeridos por ser necesarios para este fin, sin precisar del consentimiento del afectado.

2. Las entidades a las que se refiere el artículo 13 podrán tratar sin consentimiento del interesado la información que resulte imprescindible para el cumplimiento de las obligaciones establecidas en dicho precepto con la única finalidad de poner dichos datos en conocimiento de las Administraciones Públicas competentes o del Ministerio Fiscal.

3. Los datos recabados por las Administraciones Públicas podrán utilizarse única y exclusivamente para la adopción de las medidas de protección establecidas en la presente ley, atendiendo en todo caso a la garantía del interés superior del menor y sólo podrán ser comunicados a las Administraciones Públicas que hubieran de adoptar las resoluciones correspondientes, al Ministerio Fiscal y a los órganos judiciales.

4. Los datos podrán ser igualmente cedidos sin consentimiento del interesado al Ministerio Fiscal, que los tratará para el ejercicio de las funciones establecidas en esta ley y en la normativa que le es aplicable.

5. En todo caso, el tratamiento de los mencionados datos quedará sometido a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus disposición de desarrollo, siendo exigible la implantación de las medidas de seguridad de nivel alto previstas en dicha normativa.

Artículo 22 quinquies. *Impacto de las normas en la infancia y en la adolescencia.*

Las memorias del análisis de impacto normativo que deben acompañar a los anteproyectos de ley y a los proyectos de reglamentos incluirán el impacto de la normativa en la infancia y en la adolescencia.

CAPÍTULO II

De la tutela

Artículo 23. *Indices de tutelas.*

Para el ejercicio de la función de vigilancia atribuida al Ministerio Fiscal en el Código Civil respecto de la tutela asumida por la Entidad Pública por ministerio de la ley, se llevará en cada Fiscalía un Índice de Tutelas de Menores.

CAPÍTULO III

De la adopción

Artículo 24. *Adopción de menores.*

La adopción nacional e internacional se ajustará a lo establecido por la legislación civil aplicable.

CAPÍTULO IV

Centros de protección específicos de menores con problemas de conducta

Artículo 25. *Acogimiento residencial en centros de protección específicos de menores con problemas de conducta.*

1. Se someterán a las disposiciones previstas en este capítulo, los ingresos, actuaciones e intervenciones en centros de protección específicos de menores con problemas de conducta dependientes de las Entidades Públicas o de entidades privadas colaboradoras de aquellas, en los que esté prevista la utilización de medidas de seguridad y de restricción de libertades o derechos fundamentales.

Estos centros, sometidos a estándares internacionales y a control de calidad, estarán destinados al acogimiento residencial de menores que estén en situación de guarda o tutela de la Entidad Pública, diagnosticados con problemas de conducta, que presenten conductas disruptivas o di-sociales recurrentes, transgresoras de las normas sociales y los derechos de terceros, cuando además así esté justificado por sus necesidades de protección y determinado por una valoración psicosocial especializada.

2. El acogimiento residencial en estos centros se realizará exclusivamente cuando no sea posible la intervención a través de otras medidas de protección, y tendrá como finalidad proporcionar al menor un marco adecuado para su educación, la normalización de su conducta, su reintegración familiar cuando sea posible, y el libre y armónico desarrollo de su personalidad, en un contexto estructurado y con programas específicos en el marco de un proyecto educativo. Así pues, el ingreso del menor en estos centros y las medidas de seguridad que se apliquen en el mismo se utilizarán como último recurso y tendrán siempre carácter educativo.

3. En los supuestos de guarda voluntaria prevista en el artículo 19, será necesario el compromiso de la familia a someterse a la intervención profesional.

4. Estos centros dispondrán de una ratio adecuada entre el número de menores y el personal destinado a su atención para garantizar un tratamiento individualizado a cada menor.

5. En el caso de menores con discapacidad, se continuará con los apoyos especializados que vinieran recibiendo o se adoptarán otros más adecuados, incorporando en todo caso medidas de accesibilidad en los centros de ingreso y en las actuaciones que se lleven a cabo.

Artículo 26. *Ingreso en centros de protección específicos de menores con problemas de conducta.*

1. La Entidad Pública que ostente la tutela o guarda de un menor, y el Ministerio Fiscal, estarán legitimados para solicitar la autorización judicial para el ingreso del menor en los centros de protección específicos de menores con problemas de conducta. Esta solicitud de ingreso estará motivada y fundamentada en informes psicosociales emitidos previamente por personal especializado en protección de menores.

2. No podrán ser ingresados en estos centros los menores que presenten enfermedades o trastornos mentales que requieran un tratamiento específico por parte de los servicios competentes en materia de salud mental o de atención a las personas con discapacidad.

3. Para el ingreso de un menor en estos centros será necesario que la Entidad Pública o el Ministerio Fiscal recaben previamente la correspondiente autorización judicial, garantizando, en todo caso, el derecho del menor a ser oído según lo establecido en el artículo 9. Dicha autorización se otorgará tras la tramitación del procedimiento regulado en el

artículo 778 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, y deberá pronunciarse sobre la posibilidad de aplicarles medidas de seguridad, así como de limitarles temporalmente el régimen de visitas, de comunicaciones y de salidas que pudieran adoptarse.

No obstante, si razones de urgencia, convenientemente motivadas, hicieren necesaria la inmediata adopción del ingreso, la Entidad Pública o el Ministerio Fiscal podrá acordarlo previamente a la autorización judicial, debiendo comunicarlo al Juzgado competente lo antes posible y, en todo caso, dentro del plazo de veinticuatro horas, a los efectos de que se proceda a la preceptiva ratificación del mismo para lo que deberá aportar la información de que disponga y justificante del ingreso inmediato. El Juzgado resolverá en el plazo máximo de setenta y dos horas desde que reciba la comunicación, dejándose de inmediato sin efecto el ingreso en caso de que no lo autorice.

4. Los menores recibirán a su ingreso en el centro, información escrita sobre sus derechos y deberes, las normas de funcionamiento del centro, las cuestiones de organización general, el régimen educativo, el régimen disciplinario y los medios para formular peticiones, quejas y recursos. Dicha información se transmitirá de forma que se garantice su comprensión en atención a la edad y a las circunstancias del menor.

5. Los menores no permanecerán en el centro más tiempo del estrictamente necesario para atender a sus necesidades específicas. El cese será acordado por el órgano judicial que esté conociendo del ingreso, de oficio o a propuesta de la Entidad Pública o del Ministerio Fiscal. Esta propuesta estará fundamentada en un informe psicosocial.

Artículo 27. *Medidas de seguridad.*

1. Las medidas de seguridad podrán consistir en la contención del menor, en su aislamiento provisional o en registros personales y materiales. Las medidas de seguridad solo podrán utilizarse fracasadas las medidas preventivas y de desescalada, que tendrán carácter prioritario.

2. Las medidas de seguridad deberán aplicarse por personal especializado y con formación en materia de derechos de la infancia y la adolescencia, resolución de conflictos y técnicas de sujeción. Este personal solo podrá usar medidas de seguridad con los menores como último recurso, en casos de intentos de fuga, resistencia activa que suponga una alteración grave de la convivencia o una vulneración grave a los derechos de otros menores o riesgo directo de autolesión, de lesiones a otros o daños graves a las instalaciones.

3. Corresponde al Director del Centro o persona en la que este haya delegado, la adopción de decisiones sobre las medidas de seguridad, que deberán ser motivadas y habrán de notificarse con carácter inmediato a la Entidad Pública y al Ministerio Fiscal y podrán ser recurridas por el menor, el Ministerio Fiscal y la Entidad Pública, ante el órgano judicial que esté conociendo del ingreso, el cual resolverá tras recabar informe del centro y previa audiencia del menor y del Ministerio Fiscal.

4. Las medidas de seguridad aplicadas deberán registrarse en el Libro Registro de Incidencias, que será supervisado por parte de la dirección del centro.

Artículo 28. *Medidas de contención.*

1. Las medidas de contención se adoptarán en atención a las circunstancias en presencia y en la forma en que se establece en los apartados siguientes del presente artículo.

2. El personal de los centros únicamente podrá utilizar medidas de contención previo intento de restauración de la convivencia y de la seguridad a través de medidas de desescalada.

3. La contención física solo podrá consistir en la interposición entre el menor y la persona o el objeto que se encuentra en peligro, la restricción física de espacios y movimientos y, en última instancia, bajo un estricto protocolo, la inmovilización física por personal especializado del centro.

En los centros de protección específicos de menores con problemas de conducta, será admisible únicamente y con carácter excepcional la sujeción de las muñecas del menor con equipos homologados, siempre y cuando se realice bajo un estricto protocolo y no sea posible evitar por otros medios la puesta en grave riesgo de la vida o la integridad física del

menor o de terceros. Esta medida excepcional solo podrá aplicarse por el tiempo mínimo imprescindible, que no podrá ser superior a una hora. Durante este tiempo, la persona menor de edad estará acompañada presencialmente y de forma continua, o supervisada de manera permanente, por un educador u otro profesional del equipo educativo o técnico del centro.

La aplicación de esta medida se comunicará de manera inmediata a la Entidad Pública, al Ministerio Fiscal y al órgano judicial que esté conociendo del ingreso.

4. La contención mecánica está prohibida en los términos establecidos en el art. 21 ter de esta Ley.

Artículo 29. *Aislamiento del menor.*

1. El aislamiento provisional de un menor mediante su permanencia en un espacio adecuado del que se impida su salida solo podrá utilizarse en prevención de actos violentos, autolesiones, lesiones a otros menores residentes en el centro, al personal del mismo o a terceros, así como de daños graves a sus instalaciones. Se aplicará puntualmente en el momento en el que sea preciso y en ningún caso como medida disciplinaria.

2. El aislamiento no podrá exceder de tres horas consecutivas sin perjuicio del derecho al descanso del menor. Durante el periodo de tiempo en que el menor permanezca en aislamiento estará acompañado presencialmente y de forma continua o supervisado de manera permanente por un educador u otro profesional del equipo educativo o técnico del centro.

Artículo 30. *Registros personales y materiales.*

1. Los registros personales y materiales se llevarán a cabo con el respeto debido a la dignidad, privacidad y a los derechos fundamentales de la persona, con el fin de evitar situaciones de riesgo producidas por la introducción o salida del centro de objetos, instrumentos o sustancias que por sí mismos o por su uso inadecuado pueden resultar peligrosos o perjudiciales.

Se utilizarán preferentemente medios electrónicos.

2. El registro personal y cacheo del menor se efectuará por el personal indispensable que requerirá, al menos dos profesionales del centro del mismo sexo que el menor. Cuando implique alguna exposición corporal esta será parcial, se realizará en lugar adecuado, sin la presencia de otros menores y preservando en todo lo posible la intimidad del menor.

3. El personal del centro podrá realizar el registro de las pertenencias del menor, pudiendo retirarle aquellos objetos que se encuentren en su posesión que pudieran ser de ilícita procedencia, resultar dañinos para sí, para otros o para las instalaciones del centro o que no estén autorizados para menores de edad. Los registros materiales se deberán comunicar previamente al menor siempre que no pudieran efectuarse en su presencia.

Artículo 31. *Régimen disciplinario.*

1. El régimen disciplinario en estos centros se fundará siempre en el proyecto socio-educativo del centro y en el individualizado de cada menor, al cual se informará del mismo.

2. El procedimiento disciplinario será el último recurso a utilizar, dando prioridad a los sistemas restaurativos de resolución de conflictos e interacción educativa. No podrán establecerse restricciones de igual o mayor entidad que las previstas en la legislación reguladora de la responsabilidad penal de los menores.

3. En ningún caso podrán utilizarse las medidas contenidas en los artículos 27 a 30 con fines disciplinarios.

4. La regulación autonómica sobre régimen disciplinario deberá ser suficiente y adecuada a los principios de la Constitución, de esta ley y del título IX de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, garantizando al menor la asistencia legal de un abogado independiente, respetando en todo momento la dignidad y los derechos de los menores y sin que en ningún caso se les pueda privar de los mismos.

Artículo 32. *Supervisión y control.*

Con independencia de las inspecciones de los centros que puedan efectuar el Defensor del Pueblo, las instituciones autonómicas equivalentes y el Ministerio Fiscal, la medida de ingreso del menor en el centro de protección específico deberá revisarse al menos trimestralmente por la Entidad Pública, debiendo remitir al órgano judicial competente que autorizó el ingreso y al Ministerio Fiscal, con esa periodicidad, el oportuno informe motivado de seguimiento que incluya las entradas del Libro de Registro de Incidencias.

A los efectos de las inspecciones e informes a los que se refiere el párrafo anterior, el Libro de Registro de Incidencias deberá respetar, respecto a los cesionarios de datos, la adopción de las medidas de seguridad de nivel medio establecidas en la legislación vigente en materia de protección de datos de carácter personal.

Artículo 33. *Administración de medicamentos.*

1. La administración de medicamentos a los menores, cuando sea necesario para su salud, deberá tener lugar de acuerdo con la praxis profesional sanitaria, respetando las disposiciones sobre consentimiento informado, y en los términos y condiciones previstas en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

2. En todo caso, deberá ser un facultativo médico autorizado quien recete medicamentos sujetos a prescripción médica y realice el seguimiento de su correcta administración y de la evolución del tratamiento. A estos efectos se llevará un registro con la historia médica de cada uno de los menores.

Artículo 34. *Régimen de visitas y permisos de salida.*

1. Las visitas de familiares y otras personas allegadas sólo podrán ser restringidas o suspendidas en interés del menor por el Director del centro, de manera motivada, cuando su tratamiento educativo lo aconseje y conforme a los términos recogidos en la autorización judicial de ingreso.

El derecho de visitas no podrá ser restringido por la aplicación de medidas disciplinarias.

2. El Director del centro de protección específico de menores con problemas de conducta podrá restringir o suprimir las salidas de las personas ingresadas en el mismo, siempre en interés del menor y de manera motivada, cuando su tratamiento educativo lo aconseje, conforme a los términos recogidos en la autorización judicial de ingreso.

3. Las medidas limitativas del régimen de visitas y de los permisos de salida deberán ser notificadas a las personas interesadas, al menor y al Ministerio Fiscal de acuerdo con la legislación aplicable.

Dichas medidas podrán ser recurridas por el Ministerio Fiscal y por el menor al que se garantizará asistencia legal de abogado independiente, ante el órgano judicial que esté conociendo el ingreso, el cual resolverá tras recabar informe del centro y previa audiencia de las personas interesadas, del menor y del Ministerio Fiscal.

Artículo 35. *Régimen de comunicaciones del menor.*

1. Los menores ingresados en los centros tendrán derecho a remitir quejas de forma confidencial al Ministerio Fiscal, a la autoridad judicial competente y al Defensor del Pueblo o ante las instituciones autonómicas homólogas. Este derecho no podrá ser restringido por la aplicación de medidas disciplinarias.

2. Las comunicaciones del menor con familiares y otras personas allegadas serán libres y secretas.

Sólo podrán ser restringidas o suspendidas por el Director del centro en interés del menor, de manera motivada, cuando su tratamiento educativo lo aconseje y conforme a los términos recogidos en la autorización judicial de ingreso. La restricción o suspensión del derecho a mantener comunicaciones o del secreto de las mismas deberá ser adoptada de acuerdo con la legislación aplicable y notificada a las personas interesadas, al menor y al Ministerio Fiscal, quienes podrán recurrirla ante el órgano jurisdiccional que autorizó el ingreso, el cual resolverá tras recabar informe del centro y previa audiencia de las personas interesadas, del menor y del Ministerio Fiscal.

Disposición adicional primera.

Se aplicarán las normas de la jurisdicción voluntaria a las actuaciones que se sigan:

1.º Para adoptar las medidas previstas en el artículo 158 del Código Civil.
2.º Contra las resoluciones que declaren el desamparo y la asunción de la tutela por ministerio de la Ley y la idoneidad de los solicitantes de adopción.
3.º Para cualesquiera otras reclamaciones frente a resoluciones de las entidades públicas que surjan con motivo del ejercicio de sus funciones en materia de tutela o guarda de menores.

En el indicado procedimiento, los recursos se admitirán, en todo caso en un solo efecto.
Quedará siempre a salvo el ejercicio de las acciones en la vía judicial ordinaria.

Disposición adicional segunda.

Para la inscripción en el Registro español de las adopciones constituidas en el extranjero, el encargado del Registro apreciará la concurrencia de los requisitos del artículo 9.5 del Código Civil.

Disposición adicional tercera.

Con excepción de las declaraciones de incapacitación y de prodigalidad, las demás actuaciones judiciales previstas en los Títulos IX y X del Libro I del Código Civil se ajustarán al procedimiento previsto para la jurisdicción voluntaria, con las siguientes particularidades:

1.ª Tanto el Juez como el Ministerio Fiscal actuarán de oficio en interés del menor o incapaz, adoptando y proponiendo las medidas, diligencias y pruebas que estimen oportunas. Suplirán la pasividad de los particulares y les asesorarán sobre sus derechos y sobre el modo de subsanar los defectos de sus solicitudes.
2.ª No será necesaria la intervención de Abogado ni de Procurador.
3.ª La oposición de algún interesado se ventilará en el mismo procedimiento, sin convertirlo en contencioso.

Disposición transitoria única.

Los procedimientos iniciados con anterioridad a la entrada en vigor de esta Ley se regirán por la normativa anterior.

Disposición derogatoria única.

Queda derogado el Decreto de 2 de julio de 1948 por el que se aprueba el texto refundido de la Legislación sobre Protección de Menores y cuantas normas se opongan a la presente Ley.

Disposición final primera.

El artículo 9.4 del Código Civil, tendrá la siguiente redacción:

> «El carácter y contenido de la filiación, incluida la adoptiva y las relaciones paterno-filiales, se regirán por la Ley personal del hijo y si no pudiera determinarse ésta, se estará a la de la residencia habitual del hijo.»

Disposición final segunda.

El artículo 9.5 del Código Civil, párrafos tercero, cuarto y quinto, tendrá la siguiente redacción:

> «Para la constitución de la adopción, los Cónsules españoles tendrán las mismas atribuciones que el Juez, siempre que el adoptante sea español y el adoptando esté domiciliado en la demarcación consular. La propuesta previa será formulada por la entidad pública correspondiente al último lugar de residencia del adoptante en España. Si el adoptante no tuvo residencia en España en los dos últimos años, no será necesaria propuesta previa, pero el Cónsul recabará de las autoridades del lugar de residencia de aquél informes suficientes para valorar su idoneidad.

En la adopción constituida por la competente autoridad extranjera, la Ley del adoptando regirá en cuanto a capacidad y consentimientos necesarios. Los consentimientos exigidos por tal Ley podrán prestarse ante una autoridad del país en que se inició la constitución o, posteriormente, ante cualquier otra autoridad competente. En su caso, para la adopción de un español será necesario el consentimiento de la entidad pública correspondiente a la última residencia del adoptando en España.

No será reconocida en España como adopción la constituida en el extranjero por adoptante español, si los efectos de aquélla no se corresponden con los previstos por la legislación española. Tampoco lo será, mientras la entidad pública competente no haya declarado la idoneidad del adoptante, si éste fuera español y estuviera domiciliado en España al tiempo de la adopción.»

Disposición final tercera.

El artículo 149 del Código Civil, tendrá la siguiente redacción:

«El obligado a prestar alimentos podrá, a su elección, satisfacerlos, o pagando la pensión que se fije, o recibiendo y manteniendo en su propia casa al que tiene derecho a ellos.

Esta elección no será posible en cuanto contradiga la situación de convivencia determinada para el alimentista por las normas aplicables o por resolución judicial. También podrá ser rechazada cuando concurra justa causa o perjudique el interés del alimentista menor de edad.»

Disposición final cuarta.

El artículo 158 del Código Civil tendrá la siguiente redacción:

«El Juez, de oficio o a instancia del propio hijo, de cualquier pariente o del Ministerio Fiscal, dictará:

1.º Las medidas convenientes para asegurar la prestación de alimentos y proveer a las futuras necesidades del hijo, en caso de incumplimiento de este deber, por sus padres.

2.º Las disposiciones apropiadas a fin de evitar a los hijos perturbaciones dañosas en los casos de cambio de titular de la potestad de guarda.

3.º En general, las demás disposiciones que considere oportunas, a fin de apartar al menor de un peligro o de evitarle perjuicios.

Todas estas medidas podrán adoptarse dentro de cualquier proceso civil o penal o bien en un procedimiento de jurisdicción voluntaria.»

Disposición final quinta.

El artículo 172 del Código Civil queda redactado como sigue:

«1. La entidad pública a la que, en el respectivo territorio, esté encomendada la protección de los menores, cuando constate que un menor se encuentra en situación de desamparo, tiene por ministerio de la Ley la tutela del mismo y deberá adoptar las medidas de protección necesarias para su guarda, poniéndolo en conocimiento del Ministerio Fiscal, y notificando en legal forma a los padres, tutores o guardadores, en un plazo de cuarenta y ocho horas. Siempre que sea posible, en el momento de la notificación se les informará de forma presencial y de modo claro y comprensible de las causas que dieron lugar a la intervención de la Administración y de los posibles efectos de la decisión adoptada.

Se considera como situación de desamparo la que se produce de hecho a causa del incumplimiento, o del imposible o inadecuado ejercicio de los deberes de protección establecidos por las leyes para la guarda de los menores, cuando éstos queden privados de la necesaria asistencia moral o material.

La asunción de la tutela atribuida a la entidad pública lleva consigo la suspensión de la patria potestad o de la tutela ordinaria. No obstante, serán válidos los actos de contenido patrimonial que realicen los padres o tutores en representación del menor y que sean beneficiosos para él.

2. Cuando los padres o tutores, por circunstancias graves, no puedan cuidar al menor, podrán solicitar de la entidad pública competente que ésta asuma su guarda durante el tiempo necesario.

La entrega de la guarda se hará constar por escrito dejando constancia de que los padres o tutores han sido informados de las responsabilidades que siguen manteniendo respecto del hijo, así como de la forma en que dicha guarda va a ejercerse por la Administración.

Cualquier variación posterior de la forma de ejercicio será fundamentada y comunicada a aquéllos y al Ministerio Fiscal.

Asimismo, se asumirá la guarda por la entidad pública cuando así lo acuerde el Juez en los casos en que legalmente proceda.

3. La guarda asumida a solicitud de los padres o tutores o como función de la tutela por ministerio de la Ley, se realizará mediante el acogimiento familiar o el acogimiento residencial. El acogimiento familiar se ejercerá por la persona o personas que determine la entidad pública. El acogimiento residencial se ejercerá por el Director del centro donde sea acogido el menor.

4. Se buscará siempre el interés del menor y se procurará, cuando no sea contrario a ese interés, su reinserción en la propia familia y que la guarda de los hermanos se confíe a una misma institución o persona.

5. Si surgieren problemas graves de convivencia entre el menor y la persona o personas a quien hubiere sido confiado en guarda, aquél o persona interesada podrá solicitar la remoción de ésta.

6. Las resoluciones que aprecien el desamparo y declaren la asunción de la tutela por ministerio de la Ley serán recurribles ante la jurisdicción civil sin necesidad de reclamación administrativa previa.»

Disposición final sexta.

El artículo 173 del Código Civil tendrá la siguiente redacción:

«1. El acogimiento familiar produce la plena participación del menor en la vida de familia e impone a quien lo recibe las obligaciones de velar por él, tenerlo en su compañía, alimentarlo, educarlo y procurarle una formación integral. Este acogimiento se podrá ejercer por la persona o personas que sustituyan al núcleo familiar del menor o por responsable del hogar funcional.

2. El acogimiento se formalizará por escrito, con el consentimiento de la entidad pública, tenga o no la tutela o la guarda, de las personas que reciban al menor y de éste si tuviera doce años cumplidos. Cuando fueran conocidos los padres que no estuvieran privados de la patria potestad, o el tutor, será necesario también que presten o hayan prestado su consentimiento, salvo que se trate de un acogimiento familiar provisional a que hace referencia el apartado 3 de este artículo.

El documento de formalización del acogimiento familiar, a que se refiere el párrafo anterior, incluirá los siguientes extremos:

1.º Los consentimientos necesarios.

2.º Modalidad del acogimiento y duración prevista para el mismo.

3.º Los derechos y deberes de cada una de las partes, y en particular:

a) La periodicidad de las visitas por parte de la familia del menor acogido.

b) El sistema de cobertura por parte de la entidad pública o de otros responsables civiles de los daños que sufra el menor o de los que pueda causar a terceros.

c) La asunción de los gastos de manutención, educación y atención sanitaria.

4.º El contenido del seguimiento que, en función de la finalidad del acogimiento, vaya a realizar la entidad pública, y el compromiso de colaboración de la familia acogedora al mismo.

5.º La compensación económica que, en su caso, vayan a recibir los acogedores.

6.º Si los acogedores actúan con carácter profesionalizado o si el acogimiento se realiza en un hogar funcional, se señalará expresamente.

7.º Informe de los servicios de atención a menores.

Dicho documento se remitirá al Ministerio Fiscal.

3. Si los padres o el tutor no consienten o se oponen al mismo, el acogimiento sólo podrá ser acordado por el Juez, en interés del menor, conforme a los trámites de la Ley de Enjuiciamiento Civil. La propuesta de la entidad pública contendrá los mismos extremos referidos en el número anterior.

No obstante, la entidad pública podrá acordar en interés del menor, un acogimiento familiar provisional, que subsistirá hasta tanto se produzca resolución judicial.

La entidad pública, una vez realizadas las diligencias oportunas, y concluido el expediente, deberá presentar la propuesta al Juez de manera inmediata y, en todo caso, en el plazo máximo de quince días.

4. El acogimiento del menor cesará:

1.º Por decisión judicial.

2.º Por decisión de las personas que lo tienen acogido, previa comunicación de éstas a la entidad pública.

3.º A petición del tutor o de los padres que tengan la patria potestad y reclamen su compañía.

4.º Por decisión de la entidad pública que tenga la tutela o guarda del menor, cuando lo considere necesario para salvaguardar el interés de éste oídos los acogedores.

Será precisa resolución judicial de cesación cuando el acogimiento haya sido dispuesto por el Juez.

5. Todas las actuaciones de formalización y cesación del acogimiento se practicarán con la obligada reserva.»

Disposición final séptima.

Se introduce en el Código Civil un nuevo artículo con el número 173 bis, con la siguiente redacción:

«Artículo 173 bis.

El acogimiento familiar, podrá adoptar las siguientes modalidades atendiendo a su finalidad:

1.º Acogimiento familiar simple, que tendrá carácter transitorio, bien porque de la situación del menor se prevea la reinserción de éste en su propia familia bien en tanto se adopte una medida de protección que revista un carácter más estable.

2.º Acogimiento familiar permanente, cuando la edad u otras circunstancias del menor y su familia así lo aconsejen y así lo informen los servicios de atención al menor. En tal supuesto, la entidad pública podrá solicitar del Juez que atribuya a los acogedores aquellas facultades de la tutela que faciliten el desempeño de sus responsabilidades, atendiendo en todo caso al interés superior del menor.

3.º Acogimiento familiar preadoptivo, que se formalizará por la entidad pública cuando ésta eleve la propuesta de adopción del menor, informada por los servicios de atención al menor, ante la autoridad judicial, siempre que los acogedores reúnan los requisitos necesarios para adoptar, hayan sido seleccionados y hayan prestado ante la entidad pública su consentimiento a la adopción, y se encuentre el menor en situación jurídica adecuada para su adopción.

La entidad pública podrá formalizar, asimismo, un acogimiento familiar preadoptivo cuando considere, con anterioridad a la presentación de la propuesta de adopción, que fuera necesario establecer un período de adaptación del menor a la familia. Este período será lo más breve posible y, en todo caso, no podrá exceder del plazo de un año.»

Disposición final octava.

El artículo 174.2 del Código Civil queda redactado como sigue:

«2. A tal fin, la entidad pública le dará noticia inmediata de los nuevos ingresos de menores y le remitirá copia de las resoluciones administrativas y de los escritos de formalización relativos a la constitución, variación y cesación de las tutelas, guardas y acogimientos. Igualmente le dará cuenta de cualquier novedad de interés en las circunstancias del menor.

El Fiscal habrá de comprobar, al menos semestralmente, la situación del menor, y promoverá ante el Juez las medidas de protección que estime necesarias.»

Disposición final novena.

El artículo 175.1 del Código Civil queda redactado como sigue:

«1. La adopción requiere que el adoptante sea mayor de veinticinco años. En la adopción por ambos cónyuges basta que uno de ellos haya alcanzado dicha edad. En todo caso, el adoptante habrá de tener, por lo menos, catorce años más que el adoptado.»

Disposición final décima.

El artículo 176 del Código Civil quedará redactado como sigue:

«1. La adopción se constituye por resolución judicial, que tendrá en cuenta siempre el interés del adoptando y la idoneidad del adoptante o adoptantes para el ejercicio de la patria potestad.

2. Para iniciar el expediente de adopción es necesaria la propuesta previa de la entidad pública a favor del adoptante o adoptantes que dicha entidad pública haya declarado idóneos para el ejercicio de la patria potestad. La declaración de idoneidad podrá ser previa a la propuesta.

No obstante, no se requiere propuesta cuando en el adoptando concurra alguna de las circunstancias siguientes:

1.ª Ser huérfano y pariente del adoptante en tercer grado por consanguinidad o afinidad.

2.ª Ser hijo del consorte del adoptante.

3.ª Llevar más de un año acogido legalmente bajo la medida de un acogimiento preadoptivo o haber estado bajo su tutela por el mismo tiempo.

4.ª Ser mayor de edad o menor emancipado.

3. En los tres primeros supuestos del apartado anterior podrá constituirse la adopción, aunque el adoptante hubiere fallecido, si éste hubiese prestado ya ante el Juez su consentimiento. Los efectos de la resolución judicial en este caso se retrotraerán a la fecha de prestación de tal consentimiento.»

Disposición final undécima.

El artículo 177 del Código Civil quedará redactado como sigue:

«1. Habrán de consentir la adopción, en presencia del Juez, el adoptante o adoptantes y el adoptando mayor de doce años.

2. Deberán asentir a la adopción en la forma establecida en la Ley de Enjuiciamiento Civil:

1.º El cónyuge del adoptante, salvo que medie separación legal por sentencia firme o separación de hecho por mutuo acuerdo que conste fehacientemente.

2.º Los padres del adoptando que no se hallare emancipado, a menos que estuvieran privados de la patria potestad por sentencia firme o incursos en causa legal para tal privación. Esta situación sólo podrá apreciarse en procedimiento judicial contradictorio, el cual podrá tramitarse como dispone el artículo 1.827 de la Ley de Enjuiciamiento Civil.

No será necesario el asentimiento cuando los que deban prestarlo se encuentren imposibilitados para ello, imposibilidad que se apreciará motivadamente en la resolución judicial que constituya la adopción.

El asentimiento de la madre no podrá prestarse hasta que hayan transcurrido treinta días desde el parto.

3. Deberán ser simplemente oídos por el Juez:

1.º Los padres que no hayan sido privados de la patria potestad, cuando su asentimiento no sea necesario para la adopción.
2.º El tutor y, en su caso, el guardador o guardadores.
3.º El adoptando menor de doce años, si tuviere suficiente juicio.
4.º La entidad pública, a fin de apreciar la idoneidad del adoptante, cuando el adoptando lleve más de un año acogido legalmente por aquél.»

Disposición final duodécima.

El primer párrafo del artículo 211 del Código Civil tendrá la siguiente redacción:

«El internamiento por razón de trastorno psíquico, de una persona que no esté en condiciones de decidirlo por sí, aunque esté sometida a la patria potestad, requerirá autorización judicial. Esta será previa al internamiento, salvo que razones de urgencia hiciesen necesaria la inmediata adopción de la medida, de la que se dará cuenta cuanto antes al Juez y, en todo caso, dentro del plazo de veinticuatro horas. El internamiento de menores, se realizará en todo caso en un establecimiento de salud mental adecuado a su edad, previo informe de los servicios de asistencia al menor.»

Se declara inconstitucional, con el efecto establecido en el fundamento jurídico 6, por Sentencia del TC 131/2010, de 2 de diciembre. Ref. BOE-A-2011-273.

Disposición final decimotercera.

El artículo 216 del Código Civil tendrá un segundo párrafo con la siguiente redacción:

«Las medidas y disposiciones previstas en el artículo 158 de este Código podrán ser acordadas también por el Juez, de oficio o a instancia de cualquier interesado, en todos los supuestos de tutela o guarda, de hecho o de derecho, de menores e incapaces, en cuanto lo requiera el interés de éstos.»

Disposición final decimocuarta.

El artículo 234 del Código Civil tendrá un último párrafo con la siguiente redacción:

«Se considera beneficiosa para el menor la integración en la vida de familia del tutor.»

Disposición final decimoquinta.

El artículo 247 del Código Civil tendrá la siguiente redacción:

«Serán removidos de la tutela los que después de deferida incurran en causa legal de inhabilidad, o se conduzcan mal en el desempeño de la tutela, por incumplimiento de los deberes propios del cargo o por notoria ineptitud de su ejercicio, o cuando surgieran problemas de convivencia graves y continuados.»

Disposición final decimosexta.

El artículo 248 del Código Civil tendrá la siguiente redacción:

«El Juez, de oficio o a solicitud del Ministerio Fiscal, del tutelado o de otra persona interesada, decretará la remoción del tutor, previa audiencia de éste si, citado, compareciere. Asimismo, se dará audiencia al tutelado si tuviere suficiente juicio.»

Disposición final decimoséptima.

Se añade un segundo párrafo al artículo 260 del Código Civil con la siguiente redacción:

«No obstante, la entidad pública que asuma la tutela de un menor por ministerio de la Ley o la desempeñe por resolución judicial no precisará prestar fianza.»

Disposición final decimoctava.

1. Los artículos del Código Civil que se relacionan a continuación quedarán redactados como sigue:

Párrafo segundo del artículo 166:

«Los padres deberán recabar autorización judicial para repudiar la herencia o legado deferidos al hijo. Si el Juez denegase la autorización, la herencia sólo podrá ser aceptada a beneficio de inventario.»

Párrafo segundo del artículo 185:

«Serán aplicables a los representantes dativos del ausente, en cuanto se adapten a su especial representación, los preceptos que regulan el ejercicio de la tutela y las causas de inhabilidad, remoción y excusa de los tutores.»

Artículo 271:

«El tutor necesita autorización judicial:

1.º Para internar al tutelado en un establecimiento de salud mental o de educación o formación especial.

2.º Para enajenar o gravar bienes inmuebles, establecimientos mercantiles o industriales, objetos preciosos y valores mobiliarios de los menores o incapacitados, o celebrar contratos o realizar actos que tengan carácter dispositivo y sean susceptibles de inscripción. Se exceptúa la venta del derecho de suscripción preferente de acciones.

3.º Para renunciar derechos, así como transigir o someter a arbitraje cuestiones en que el tutelado estuviese interesado.

4.º Para aceptar sin beneficio de inventario cualquier herencia, o para repudiar ésta o las liberalidades.

5.º Para hacer gastos extraordinarios en los bienes.

6.º Para entablar demanda en nombre de los sujetos a tutela, salvo en los asuntos urgentes o de escasa cuantía.

7.º Para ceder bienes en arrendamiento por tiempo superior a seis años.

8.º Para dar y tomar dinero a préstamo.

9.º Para disponer a título gratuito de bienes o derechos del tutelado.

10. Para ceder a terceros los créditos que el tutelado tenga contra él, o adquirir a título oneroso los créditos de terceros contra el tutelado.»

Artículo 272:

«No necesitarán autorización judicial la partición de herencia ni la división de cosa común realizadas por el tutor, pero una vez practicadas requerirán aprobación judicial.»

Artículo 273:

«Antes de autorizar o aprobar cualquiera de los actos comprendidos en los dos artículos anteriores, el Juez oirá al Ministerio Fiscal y al tutelado, si fuese mayor de doce años o lo considera oportuno, y recabará los informes que le sean solicitados o estime pertinentes.»

Artículo 300:

«El Juez, en procedimiento de jurisdicción voluntaria, de oficio o a petición del Ministerio Fiscal, del propio menor o de cualquier persona capaz de comparecer en juicio, nombrará defensor a quien estime más idóneo para el cargo.»

Artículo 753:

«Tampoco surtirá efecto la disposición testamentaria en favor de quien sea tutor o curador del testador, salvo cuando se haya hecho después de aprobadas definitivamente las cuentas o, en el caso en que no tuviese que rendirse éstas, después de la extinción de la tutela o curatela.

Serán, sin embargo, válidas las disposiciones hechas en favor del tutor o curador que sea ascendiente, descendiente, hermano, hermana o cónyuge del testador.»

Artículo 996:
«Si la sentencia de incapacitación por enfermedades o deficiencias físicas o psíquicas no dispusiere otra cosa, el sometido a curatela podrá, asistido del curador, aceptar la herencia pura y simplemente o a beneficio de inventario.»

Párrafo tercero del artículo 1.057:
«Lo dispuesto en este artículo y en el anterior se observará aunque entre los coherederos haya alguno sometido a patria potestad o tutela, o a curatela por prodigalidad o por enfermedades o deficiencias físicas o psíquicas; pero el contador partidor deberá en estos casos inventariar los bienes de la herencia, con citación de los representantes legales o curadores de dichas personas.»

Artículo 1.329:
«El menor no emancipado que con arreglo a la Ley pueda casarse podrá otorgar capitulaciones, pero necesitará el concurso y consentimiento de sus padres o tutor, salvo que se limite a pactar el régimen de separación o el de participación.»

Artículo 1.330:
«El incapacitado judicialmente sólo podrá otorgar capitulaciones matrimoniales con la asistencia de sus padres, tutor o curador.»

Número 1.º del artículo 1.459:
«Los que desempeñen algún cargo tutelar, los bienes de la persona o personas que estén bajo su guarda o protección.»

Número 3.º del artículo 1.700:
«Por muerte, insolvencia, incapacitación o declaración de prodigalidad de cualquiera de los socios, y en el caso previsto en el artículo 1.699.»

Número 3.º del artículo 1.732:
«Por muerte, incapacitación, declaración de prodigalidad, quiebra o insolvencia del mandante o del mandatario.»

2. Quedan modificados los siguientes artículos del Código Civil:

En los artículos 108, 823 y 980 quedan suprimidas, respectivamente, las palabras «plena», «plena» y «plenamente».

En los artículos 323 y 324 se sustituyen, respectivamente, las palabras «tutor» y «tutores» por «curador» y «curadores».

Queda suprimido el párrafo tercero del artículo 163.

En el primer párrafo del artículo 171 se eliminan las palabras «no se constituirá la tutela, sino que».

Al final del último párrafo de este mismo artículo 171 se agrega la frase «o curatela, según proceda».

El número 1.º del artículo 234 se sustituye por el siguiente:

«Al cónyuge que conviva con el tutelado.»

En el artículo 852 se sustituye «y 5.º» por «, 5.º y 6.º».

En el artículo 855 se sustituye «y 6.º» por «, 5.º y 6.º»; «169» por «170», y se suprime su último párrafo.

Queda suprimido el párrafo segundo del artículo 992 y en el tercero, que pasará a ser segundo, se elimina la palabra «también».

Se agrega un segundo párrafo al artículo 1.060 del siguiente tenor:

«El defensor judicial designado para representar a un menor o incapacitado en una partición, deberá obtener la aprobación del Juez, si éste no hubiera dispuesto otra cosa al hacer el nombramiento.»

El número 2.º del artículo 1.263 queda sustituido por el siguiente:

«Los incapacitados.»

En el número 1.º del artículo 1.291 las palabras «sin autorización judicial» sustituyen a «sin autorización del consejo de familia».

En el artículo 1.338 se sustituyen las palabras «El menor» por «El menor no emancipado».

En el número 1.º del artículo 1.393 se sustituyen las palabras «declarado ausente» por «declarado pródigo, ausente».

Disposición final decimonovena.

La Ley de Enjuiciamiento Civil quedará modificada en el siguiente sentido:

1. Los actuales artículos 1.910 a 1.918 de la Ley de Enjuiciamiento Civil pasarán a integrar la Sección Tercera del Título IV del Libro III, titulada «Medidas provisionales en relación con los hijos de familia».

2. La Sección Segunda del Título IV del Libro III, se denominará «Medidas relativas al retorno de menores en los supuestos de sustracción internacional» y comprenderá los artículos 1.901 a 1.909, ambos inclusive, con el siguiente contenido:

«Artículo 1901

En los supuestos en que, siendo aplicable un convenio internacional, se pretenda la restitución de un menor que hubiera sido objeto de un traslado o retención ilícita, se procederá de acuerdo con lo previsto en esta Sección.

Artículo 1902

Será competente el Juez de Primera Instancia en cuya demarcación judicial se halle el menor que ha sido objeto de un traslado o retención ilícitos.

Podrá promover el procedimiento la persona, institución u organismo que tenga atribuido el derecho de custodia del menor, la autoridad central española encargada del cumplimiento de las obligaciones impuestas por el correspondiente convenio y, en representación de ésta, la persona que designe dicha autoridad.

Las actuaciones se practicarán con intervención del Ministerio Fiscal y los interesados podrán actuar bajo la dirección de Abogado.

La tramitación del procedimiento tendrá carácter preferente y deberá realizarse en el plazo de seis semanas desde la fecha en que se hubiere solicitado ante el Juez la restitución del menor.

Artículo 1903

A petición de quien promueva el procedimiento o del Ministerio Fiscal, el Juez podrá adoptar la medida provisional de custodia del menor prevista en la Sección siguiente de esta Ley y cualquier otra medida de aseguramiento que estime pertinente.

Artículo 1904

Promovido el expediente mediante la solicitud a la que se acompañará la documentación requerida por el correspondiente convenio internacional, el Juez dictará, en el plazo de veinticuatro horas, resolución en la que se requerirá a la persona que ha sustraído o retiene al menor, con los apercibimientos legales, para que en la fecha que se determine, que no podrá exceder de los tres días siguientes, comparezca en el juzgado con el menor y manifieste:

a) Si accede voluntariamente a la restitución del menor a la persona, institución y organismo que es titular del derecho de custodia; o, en otro caso,

b) Si se opone a la restitución por existir alguna de las causas establecidas en el correspondiente convenio cuyo texto se acompañará al requerimiento.

Artículo 1905

Si no compareciese el requerido, el Juez dispondrá a continuación del procedimiento de su rebeldía citando a los interesados y al Ministerio Fiscal a una

comparecencia que tendrá lugar en plazo no superior a los cinco días siguientes y decretará las medidas provisionales que juzgue pertinentes en relación con el menor.

En la comparecencia se oirá al solicitante y al Ministerio Fiscal y en su caso y separadamente, al menor sobre su restitución. El Juez resolverá por auto dentro de los dos días siguientes a contar desde la fecha de la comparecencia, si procede o no la restitución, teniendo en cuenta el interés del menor y los términos del correspondiente convenio.

Artículo 1906

Si compareciese el requerido y accediere a la restitución voluntaria del menor, se levantará acta, acordando el Juez, mediante auto, la conclusión del procedimiento y la entrega del menor a la persona, institución y organismo titular del derecho de custodia, así como lo procedente en cuanto a costas y gastos.

Artículo 1907

Si en la primera comparecencia el requerido formulase oposición a la restitución del menor, al amparo de las causas establecidas en el correspondiente convenio, no será de aplicación lo dispuesto en el artículo 1.817 de esta Ley, ventilándose la oposición ante el mismo Juez por los trámites del juicio verbal. A este fin:

a) En el mismo acto de comparecencia serán citados todos los interesados y el Ministerio Fiscal, para que expongan lo que estimen procedente y, en su caso, se practiquen las pruebas, en ulterior comparecencia, que se celebrará de conformidad con lo dispuesto en el artículo 730 y concordantes de esta Ley dentro del plazo improrrogable de los cinco días a contar desde la primera.

b) Asimismo, tras la primera comparecencia el Juez oirá, en su caso, separadamente al menor sobre su restitución y podrá recabar los informes que estime pertinentes.

Artículo 1908

Celebrada la comparecencia y, en su caso, practicadas las pruebas pertinentes dentro de los seis días posteriores, el Juez dictará auto dentro de los tres días siguientes, resolviendo, en interés del menor y en los términos del convenio, si procede o no su restitución. Contra dicho auto sólo cabrá recurso de apelación en un solo efecto, que deberá resolverse en el improrrogable plazo de veinte días.

Artículo 1909

Si el Juez resolviese la restitución del menor, en el auto se establecerá que la persona que trasladó o retuvo al menor abone las costas del procedimiento así como los gastos en que haya incurrido el solicitante, incluídos los del viaje y los que ocasione la restitución del menor al Estado de su residencia habitual con anterioridad a la sustracción, que se harán efectivos por los trámites previstos en el artículo 928 y concordantes de esta Ley.

En los demás supuestos, se declararán de oficio las costas del procedimiento.»

Disposición final vigésima.

El Ministerio Fiscal velará para que, incoado un procedimiento sobre reclamación frente a las resoluciones de las entidades públicas que surjan con motivo del ejercicio de sus funciones en materia de tutela o de guarda, se resuelvan en el mismo expediente todas las acciones e incidencias que afecten a un mismo menor. A tal efecto, promoverá ante los órganos jurisdiccionales las actuaciones oportunas previstas en la legislación procesal.

Disposición final vigésima primera.

1. El artículo 5, en sus apartados 3 y 4; el artículo 7 en su apartado 1; el artículo 8, en su apartado 2 letra c); el artículo 10, en sus apartados 1 y 2 letras a), b) y d); los artículos 11,

12, 13, 15, 16, 17, 18 en su apartado 2, 21 en sus apartados 1, 2 y 3, y el artículo 22, son legislación supletoria de la que dicten las Comunidades Autónomas con competencia en materia de asistencia social.

2. El artículo 10, en su apartado 3, el artículo 21, en su apartado 4, el artículo 23, las disposiciones adicionales primera, segunda y tercera, la disposición transitoria única y las disposiciones finales decimonovena y vigésima, se dictan al amparo del artículo 149.1.2.ª, 5.ª y 6.ª de la Constitución.

3. Los restantes preceptos no orgánicos de la Ley, así como las revisiones al Código Civil contenidas en la misma, se dictan al amparo del artículo 149.1.8.ª de la Constitución y se aplicarán sin perjuicio de la normativa que dicten las Comunidades Autónomas con competencia en materia de Derecho Civil, Foral o Especial.

Disposición final vigésima segunda.

Las entidades públicas mencionadas en esta Ley son las designadas por las Comunidades Autónomas y las ciudades de Ceuta y Melilla, de acuerdo con sus respectivas normas de organización.

Disposición final vigésima tercera.

Tienen carácter de ley ordinaria los artículos 1; 5, apartados 3 y 4; 7, apartado 1; 8, apartado 2, párrafo c; 9 bis; 9 ter; 9 quáter; 9 quinquies; 10, apartados 1, 2, párrafos a, b, d y f, 3, 4 y 5; 11, 12, 13, 14, 15, 16, 17, 18, 19, 19 bis, 20, 20 bis, 21, 21 bis, 22, 22 bis, 22 ter, 22 quáter, 22 quinquies, 23 y 24; las disposiciones adicionales primera, segunda y tercera; la disposición transitoria; la disposición derogatoria, y las disposiciones finales primera a vigésima segunda y vigésima cuarta.

Los preceptos relacionados en el párrafo anterior se aplicarán según lo previsto en la disposición final vigésima primera.

Disposición final vigésima cuarta.

La presente Ley entrará en vigor a los treinta días de su publicación en el «Boletín Oficial del Estado».

§ 30

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Jefatura del Estado
«BOE» núm. 274, de 15 de noviembre de 2002
Última modificación: 5 de junio de 2021
Referencia: BOE-A-2002-22188

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

La importancia que tienen los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales se pone de manifiesto al constatar el interés que han demostrado por los mismos casi todas las organizaciones internacionales con competencia en la materia. Ya desde el fin de la Segunda Guerra Mundial, organizaciones como Naciones Unidas, UNESCO o la Organización Mundial de la Salud, o, más recientemente, la Unión Europea o el Consejo de Europa, entre muchas otras, han impulsado declaraciones o, en algún caso, han promulgado normas jurídicas sobre aspectos genéricos o específicos relacionados con esta cuestión. En este sentido, es necesario mencionar la trascendencia de la Declaración universal de derechos humanos, del año 1948, que ha sido el punto de referencia obligado para todos los textos constitucionales promulgados posteriormente o, en el ámbito más estrictamente sanitario, la Declaración sobre la promoción de los derechos de los pacientes en Europa, promovida el año 1994 por la Oficina Regional para Europa de la Organización Mundial de la Salud, aparte de múltiples declaraciones internacionales de mayor o menor alcance e influencia que se han referido a dichas cuestiones.

Últimamente, cabe subrayar la relevancia especial del Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina (Convenio sobre los derechos del hombre y la biomedicina), suscrito el día 4 de abril de 1997, el cual ha entrado en vigor en el Reino de España el 1 de enero de 2000. Dicho Convenio es una iniciativa capital: en efecto, a diferencia de las distintas declaraciones internacionales que lo han precedido, es el primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben. Su especial valía reside en el hecho de que establece un marco común para la protección de los derechos humanos y la dignidad humana en la aplicación de la biología y la medicina. El

Convenio trata explícitamente, con detenimiento y extensión, sobre la necesidad de reconocer los derechos de los pacientes, entre los cuales resaltan el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas, persiguiendo el alcance de una armonización de las legislaciones de los diversos países en estas materias; en este sentido, es absolutamente conveniente tener en cuenta el Convenio en el momento de abordar el reto de regular cuestiones tan importantes.

Es preciso decir, sin embargo, que la regulación del derecho a la protección de la salud, recogido por el artículo 43 de la Constitución de 1978, desde el punto de vista de las cuestiones más estrechamente vinculadas a la condición de sujetos de derechos de las personas usuarias de los servicios sanitarios, es decir, la plasmación de los derechos relativos a la información clínica y la autonomía individual de los pacientes en lo relativo a su salud, ha sido objeto de una regulación básica en el ámbito del Estado, a través de la Ley 14/1986, de 25 de abril, General de Sanidad.

De otra parte, esta Ley, a pesar de que fija básicamente su atención en el establecimiento y ordenación del sistema sanitario desde un punto de vista organizativo, dedica a esta cuestión diversas previsiones, entre las que destaca la voluntad de humanización de los servicios sanitarios. Así mantiene el máximo respeto a la dignidad de la persona y a la libertad individual, de un lado, y, del otro, declara que la organización sanitaria debe permitir garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación.

A partir de dichas premisas, la presente Ley completa las previsiones que la Ley General de Sanidad enunció como principios generales. En este sentido, refuerza y da un trato especial al derecho a la autonomía del paciente. En particular, merece mención especial la regulación sobre instrucciones previas que contempla, de acuerdo con el criterio establecido en el Convenio de Oviedo, los deseos del paciente expresados con anterioridad dentro del ámbito del consentimiento informado. Asimismo, la Ley trata con profundidad todo lo referente a la documentación clínica generada en los centros asistenciales, subrayando especialmente la consideración y la concreción de los derechos de los usuarios en este aspecto.

En septiembre de 1997, en desarrollo de un convenio de colaboración entre el Consejo General del Poder Judicial y el Ministerio de Sanidad y Consumo, tuvo lugar un seminario conjunto sobre información y documentación clínica, en el que se debatieron los principales aspectos normativos y judiciales en la materia. Al mismo tiempo, se constituyó un grupo de expertos a quienes se encargó la elaboración de unas directrices para el desarrollo futuro de este tema. Este grupo suscribió un dictamen el 26 de noviembre de 1997, que ha sido tenido en cuenta en la elaboración de los principios fundamentales de esta Ley.

La atención que a estas materias otorgó en su día la Ley General de Sanidad supuso un notable avance como reflejan, entre otros, sus artículos 9, 10 y 61. Sin embargo, el derecho a la información, como derecho del ciudadano cuando demanda la atención sanitaria, ha sido objeto en los últimos años de diversas matizaciones y ampliaciones por Leyes y disposiciones de distinto tipo y rango, que ponen de manifiesto la necesidad de una reforma y actualización de la normativa contenida en la Ley General de Sanidad. Así, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión.

Esta defensa de la confidencialidad había sido ya defendida por la Directiva comunitaria 95/46, de 24 de octubre, en la que, además de reafirmarse la defensa de los derechos y libertades de los ciudadanos europeos, en especial de su intimidad relativa a la información relacionada con su salud, se apunta la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. Se manifiesta así una concepción comunitaria del derecho a la salud, en la que, junto al interés singular de cada

individuo, como destinatario por excelencia de la información relativa a la salud, aparecen también otros agentes y bienes jurídicos referidos a la salud pública, que deben ser considerados, con la relevancia necesaria, en una sociedad democrática avanzada. En esta línea, el Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general.

Todas estas circunstancias aconsejan una adaptación de la Ley General de Sanidad con el objetivo de aclarar la situación jurídica y los derechos y obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias. Se trata de ofrecer en el terreno de la información y la documentación clínicas las mismas garantías a todos los ciudadanos del Estado, fortaleciendo con ello el derecho a la protección de la salud que reconoce la Constitución.

CAPÍTULO I

Principios generales

Artículo 1. *Ámbito de aplicación.*

La presente Ley tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica.

Artículo 2. *Principios básicos.*

1. La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica.
2. Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley.
3. El paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles.
4. Todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados en la Ley. Su negativa al tratamiento constará por escrito.
5. Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria.
6. Todo profesional que interviene en la actividad asistencial está obligado no sólo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y de documentación clínica, y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente.
7. La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida.

Artículo 3. *Las definiciones legales.*

A efectos de esta Ley se entiende por:

Centro sanitario: el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios.

Certificado médico: la declaración escrita de un médico que da fe del estado de salud de una persona en un determinado momento.

Consentimiento informado: la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud.

Documentación clínica: el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.

Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Información clínica: todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.

Informe de alta médica: el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas.

Intervención en el ámbito de la sanidad: toda actuación realizada con fines preventivos, diagnósticos, terapéuticos, rehabilitadores o de investigación.

Libre elección: la facultad del paciente o usuario de optar, libre y voluntariamente, entre dos o más alternativas asistenciales, entre varios facultativos o entre centros asistenciales, en los términos y condiciones que establezcan los servicios de salud competentes, en cada caso.

Médico responsable: el profesional que tiene a su cargo coordinar la información y la asistencia sanitaria del paciente o del usuario, con el carácter de interlocutor principal del mismo en todo lo referente a su atención e información durante el proceso asistencial, sin perjuicio de las obligaciones de otros profesionales que participan en las actuaciones asistenciales.

Paciente: la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud.

Servicio sanitario: la unidad asistencial con organización propia, dotada de los recursos técnicos y del personal cualificado para llevar a cabo actividades sanitarias.

Usuario: la persona que utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria.

CAPÍTULO II

El derecho de información sanitaria

Artículo 4. *Derecho a la información asistencial.*

1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias.

2. La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar decisiones de acuerdo con su propia y libre voluntad.

3. El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle.

Artículo 5. *Titular del derecho a la información asistencial.*

1. El titular del derecho a la información es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita.

2. El paciente será informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal.

3. Cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho.

4. El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave.

Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho.

Artículo 6. *Derecho a la información epidemiológica.*

Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley.

CAPÍTULO III

Derecho a la intimidad

Artículo 7. *El derecho a la intimidad.*

1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

CAPÍTULO IV

El respeto de la autonomía del paciente

Artículo 8. *Consentimiento informado.*

1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso.

2. El consentimiento será verbal por regla general.

Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.

3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos.

4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud.

5. El paciente puede revocar libremente por escrito su consentimiento en cualquier momento.

Artículo 9. *Límites del consentimiento informado y consentimiento por representación.*

1. La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención.

2. Los facultativos podrán llevar a cabo las intervenciones clínicas indispensables en favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos:

a) Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas.

b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él.

3. Se otorgará el consentimiento por representación en los siguientes supuestos:

a) Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho.

b) Cuando el paciente tenga la capacidad modificada judicialmente y así conste en la sentencia.

c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor, después de haber escuchado su opinión, conforme a lo dispuesto en el artículo 9 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

4. Cuando se trate de menores emancipados o mayores de 16 años que no se encuentren en los supuestos b) y c) del apartado anterior, no cabe prestar el consentimiento por representación.

No obstante lo dispuesto en el párrafo anterior, cuando se trate de una actuación de grave riesgo para la vida o salud del menor, según el criterio del facultativo, el consentimiento lo prestará el representante legal del menor, una vez oída y tenida en cuenta la opinión del mismo.

5. La práctica de ensayos clínicos y la práctica de técnicas de reproducción humana asistida se rigen por lo establecido con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación.

Para la interrupción voluntaria del embarazo de menores de edad o personas con capacidad modificada judicialmente será preciso, además de su manifestación de voluntad, el consentimiento expreso de sus representantes legales. En este caso, los conflictos que surjan en cuanto a la prestación del consentimiento por parte de los representantes legales, se resolverán de conformidad con lo dispuesto en el Código Civil.

6. En los casos en los que el consentimiento haya de otorgarlo el representante legal o las personas vinculadas por razones familiares o de hecho en cualquiera de los supuestos descritos en los apartados 3 a 5, la decisión deberá adoptarse atendiendo siempre al mayor beneficio para la vida o salud del paciente. Aquellas decisiones que sean contrarias a dichos intereses deberán ponerse en conocimiento de la autoridad judicial, directamente o a través del Ministerio Fiscal, para que adopte la resolución correspondiente, salvo que, por razones de urgencia, no fuera posible recabar la autorización judicial, en cuyo caso los profesionales sanitarios adoptarán las medidas necesarias en salvaguarda de la vida o salud del paciente, amparados por las causas de justificación de cumplimiento de un deber y de estado de necesidad.

7. La prestación del consentimiento por representación será adecuada a las circunstancias y proporcionada a las necesidades que haya que atender, siempre en favor

del paciente y con respeto a su dignidad personal. El paciente participará en la medida de lo posible en la toma de decisiones a lo largo del proceso sanitario. Si el paciente es una persona con discapacidad, se le ofrecerán las medidas de apoyo pertinentes, incluida la información en formatos adecuados, siguiendo las reglas marcadas por el principio del diseño para todos de manera que resulten accesibles y comprensibles a las personas con discapacidad, para favorecer que pueda prestar por sí su consentimiento.

Artículo 10. *Condiciones de la información y consentimiento por escrito.*

1. El facultativo proporcionará al paciente, antes de recabar su consentimiento escrito, la información básica siguiente:

a) Las consecuencias relevantes o de importancia que la intervención origina con seguridad.
b) Los riesgos relacionados con las circunstancias personales o profesionales del paciente.
c) Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención.
d) Las contraindicaciones.

2. El médico responsable deberá ponderar en cada caso que cuanto más dudoso sea el resultado de una intervención más necesario resulta el previo consentimiento por escrito del paciente.

Artículo 11. *Instrucciones previas.*

1. Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas.
2. Cada servicio de salud regulará el procedimiento adecuado para que, llegado el caso, se garantice el cumplimiento de las instrucciones previas de cada persona, que deberán constar siempre por escrito.
3. No serán aplicadas las instrucciones previas contrarias al ordenamiento jurídico, a la «lex artis», ni las que no se correspondan con el supuesto de hecho que el interesado haya previsto en el momento de manifestarlas. En la historia clínica del paciente quedará constancia razonada de las anotaciones relacionadas con estas previsiones.
4. Las instrucciones previas podrán revocarse libremente en cualquier momento dejando constancia por escrito.
5. Con el fin de asegurar la eficacia en todo el territorio nacional de las instrucciones previas manifestadas por los pacientes y formalizadas de acuerdo con lo dispuesto en la legislación de las respectivas Comunidades Autónomas, se creará en el Ministerio de Sanidad y Consumo el Registro nacional de instrucciones previas que se regirá por las normas que reglamentariamente se determinen, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud.

Artículo 12. *Información en el Sistema Nacional de Salud.*

1. Además de los derechos reconocidos en los artículos anteriores, los pacientes y los usuarios del Sistema Nacional de Salud tendrán derecho a recibir información sobre los servicios y unidades asistenciales disponibles, su calidad y los requisitos de acceso a ellos.
2. Los servicios de salud dispondrán en los centros y servicios sanitarios de una guía o carta de los servicios en la que se especifiquen los derechos y obligaciones de los usuarios, las prestaciones disponibles, las características asistenciales del centro o del servicio, y sus dotaciones de personal, instalaciones y medios técnicos.

Se facilitará a todos los usuarios información sobre las guías de participación y sobre sugerencias y reclamaciones.

3. Cada servicio de salud regulará los procedimientos y los sistemas para garantizar el efectivo cumplimiento de las previsiones de este artículo.

Artículo 13. *Derecho a la información para la elección de médico y de centro.*

Los usuarios y pacientes del Sistema Nacional de Salud, tanto en la atención primaria como en la especializada, tendrán derecho a la información previa correspondiente para elegir médico, e igualmente centro, con arreglo a los términos y condiciones que establezcan los servicios de salud competentes.

CAPÍTULO V

La historia clínica

Artículo 14. *Definición y archivo de la historia clínica.*

1. La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

2. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

3. Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.

4. Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

Artículo 15. *Contenido de la historia clínica de cada paciente.*

1. La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

2. La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud.

El contenido mínimo de la historia clínica será el siguiente:

a) La documentación relativa a la hoja clínicoestadística.
b) La autorización de ingreso.
c) El informe de urgencia.
d) La anamnesis y la exploración física.
e) La evolución.
f) Las órdenes médicas.
g) La hoja de interconsulta.
h) Los informes de exploraciones complementarias.
i) El consentimiento informado.
j) El informe de anestesia.
k) El informe de quirófano o de registro del parto.
l) El informe de anatomía patológica.
m) La evolución y planificación de cuidados de enfermería.
n) La aplicación terapéutica de enfermería.

ñ) El gráfico de constantes.
o) El informe clínico de alta.

Los párrafos b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga.

3. Cuando se trate del nacimiento, la historia clínica incorporará, además de la información a la que hace referencia este apartado, los resultados de las pruebas biométricas, médicas o analíticas que resulten, en su caso, necesarias para determinar el vínculo de filiación con la madre, en los términos que se establezcan reglamentariamente.

4. La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial.

5. Cuando la atención sanitaria prestada lo sea a consecuencia de violencia ejercida contra personas menores de edad, la historia clínica especificará esta circunstancia, además de la información a la que hace referencia este apartado.

Artículo 16. *Usos de la historia clínica.*

1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.

Artículo 17. *La conservación de la documentación clínica.*

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

No obstante, los datos de la historia clínica relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración correspondiente, donde se conservarán con las debidas medidas de seguridad a los efectos de la legislación de protección de datos.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Sin perjuicio del derecho al que se refiere el artículo siguiente, los datos de la historia clínica relacionados con las pruebas biométricas, médicas o analíticas que resulten necesarias para determinar el vínculo de filiación con la madre del recién nacido, sólo podrán ser comunicados a petición judicial, dentro del correspondiente proceso penal o en caso de reclamación o impugnación judicial de la filiación materna.

3. Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes.

4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

6. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Artículo 18. *Derechos de acceso a la historia clínica.*

1. El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.

2. El derecho de acceso del paciente a la historia clínica puede ejercerse también por representación debidamente acreditada.

3. El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

4. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que

afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

Artículo 19. *Derechos relacionados con la custodia de la historia clínica.*

El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley.

CAPÍTULO VI

Informe de alta y otra documentación clínica

Artículo 20. *Informe de alta.*

Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas.

Artículo 21. *El alta del paciente.*

1. En caso de no aceptar el tratamiento prescrito, se propondrá al paciente o usuario la firma del alta voluntaria. Si no la firmara, la dirección del centro sanitario, a propuesta del médico responsable, podrá disponer el alta forzosa en las condiciones reguladas por la Ley.

El hecho de no aceptar el tratamiento prescrito no dará lugar al alta forzosa cuando existan tratamientos alternativos, aunque tengan carácter paliativo, siempre que los preste el centro sanitario y el paciente acepte recibirlos. Estas circunstancias quedarán debidamente documentadas.

2. En el caso de que el paciente no acepte el alta, la dirección del centro, previa comprobación del informe clínico correspondiente, oirá al paciente y, si persiste en su negativa, lo pondrá en conocimiento del juez para que confirme o revoque la decisión.

Artículo 22. *Emisión de certificados médicos.*

Todo paciente o usuario tiene derecho a que se le faciliten los certificados acreditativos de su estado de salud. Éstos serán gratuitos cuando así lo establezca una disposición legal o reglamentaria.

Artículo 23. *Obligaciones profesionales de información técnica, estadística y administrativa.*

Los profesionales sanitarios, además de las obligaciones señaladas en materia de información clínica, tienen el deber de cumplimentar los protocolos, registros, informes, estadísticas y demás documentación asistencial o administrativa, que guarden relación con los procesos clínicos en los que intervienen, y los que requieran los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica.

Disposición adicional primera. *Carácter de legislación básica.*

Esta Ley tiene la condición de básica, de conformidad con lo establecido en el artículo 149.1.1.ª y 16.ª de la Constitución.

El Estado y las Comunidades Autónomas adoptarán, en el ámbito de sus respectivas competencias, las medidas necesarias para la efectividad de esta Ley.

Disposición adicional segunda. *Aplicación supletoria.*

Las normas de esta Ley relativas a la información asistencial, la información para el ejercicio de la libertad de elección de médico y de centro, el consentimiento informado del paciente y la documentación clínica, serán de aplicación supletoria en los proyectos de

investigación médica, en los procesos de extracción y trasplante de órganos, en los de aplicación de técnicas de reproducción humana asistida y en los que carezcan de regulación especial.

Disposición adicional tercera. *Coordinación de las historias clínicas.*

El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

Disposición adicional cuarta. *Necesidades asociadas a la discapacidad.*

El Estado y las Comunidades Autónomas, dentro del ámbito de sus respectivas competencias, dictarán las disposiciones precisas para garantizar a los pacientes o usuarios con necesidades especiales, asociadas a la discapacidad, los derechos en materia de autonomía, información y documentación clínica regulados en esta Ley.

Disposición adicional quinta. *Información y documentación sobre medicamentos y productos sanitarios.*

La información, la documentación y la publicidad relativas a los medicamentos y productos sanitarios, así como el régimen de las recetas y de las órdenes de prescripción correspondientes, se regularán por su normativa específica, sin perjuicio de la aplicación de las reglas establecidas en esta Ley en cuanto a la prescripción y uso de medicamentos o productos sanitarios durante los procesos asistenciales.

Disposición adicional sexta. *Régimen sancionador.*

Las infracciones de lo dispuesto por la presente Ley quedan sometidas al régimen sancionador previsto en el capítulo VI del Título I de la Ley 14/1986, General de Sanidad, sin perjuicio de la responsabilidad civil o penal y de la responsabilidad profesional o estatutaria procedentes en derecho.

Disposición transitoria única. *Informe de alta.*

El informe de alta se regirá por lo dispuesto en la Orden del Ministerio de Sanidad, de 6 de septiembre de 1984, mientras no se desarrolle legalmente lo dispuesto en el artículo 20 de esta Ley.

Disposición derogatoria única. *Derogación general y de preceptos concretos.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Ley y, concretamente, los apartados 5, 6, 8, 9 y 11 del artículo 10, el apartado 4 del artículo 11 y el artículo 61 de la Ley 14/1986, General de Sanidad.

Disposición final única. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de seis meses a partir del día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 31

Ley 5/2002, de 4 de abril, reguladora de los Boletines Oficiales de las Provincias

Jefatura del Estado
«BOE» núm. 82, de 5 de abril de 2002
Última modificación: sin modificaciones
Referencia: BOE-A-2002-6467

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

Los Boletines Oficiales de la Provincia se crean por Real Orden de 20 de abril de 1833, donde se establece en cada capital de provincia un diario o boletín periódico en el que se insertarían todas las órdenes, disposiciones y prevenciones que tuvieran que hacerse a las justicias y Ayuntamientos de los pueblos por cualquier autoridad.

La citada norma creó y generalizó los boletines oficiales para todas las provincias, pero no especificó la organización administrativa responsable de su edición y coste económico, así como de la dirección y ordenación de las inserciones de disposiciones y anuncios.

Con posterioridad surgen numerosas disposiciones (Reales Órdenes de 26 de marzo de 1837, 5 de julio de 1837, 6 de abril de 1839, 4 de abril de 1840, 24 de mayo de 1846, 3 de septiembre de 1846, 21 de enero de 1849, 15 de julio de 1849 y 8 de octubre de 1856) que completan la Real Orden de creación de estos boletines oficiales, atribuyendo a los entonces Jefes Políticos la responsabilidad de la edición de los mismos, siendo los órganos decisorios para la inserción de los correspondientes textos, atribuciones éstas que obedecían a su configuración como agentes estatales de comunicación y control de las provincias y de las autoridades locales, a quienes trasladaban las disposiciones dictadas por el Gobierno, verificando su obligado cumplimiento.

A partir de las Reales Órdenes de 8 de octubre de 1856 y de 1 de agosto de 1871, la gestión material del servicio de edición de los Boletines Oficiales de la Provincia pasa a ser responsabilidad de las Diputaciones Provinciales quienes, además, asumían el coste de tal edición, que pasó a considerarse como obligación de dichas Entidades.

II

Esta regulación de los Boletines Oficiales de la Provincia ha dado lugar, desde hace largo tiempo, a diversos problemas derivados, fundamentalmente, de la falta de adecuación de esta normativa a la nueva configuración territorial del Estado, lo que ha llevado a la existencia de un consenso generalizado en torno a la necesidad de una reforma legal que clarifique definitivamente esta cuestión nuclear y, con ello, el régimen de gestión de este servicio.

La disposición adicional quinta de la Ley 25/1998, de 13 de julio, de modificación del Régimen Legal de las Tasas Estatales y Locales y de Reordenación de las Prestaciones Patrimoniales de Carácter Público, dio una nueva redacción al artículo 122 de la Ley 39/1988, de 28 de diciembre, reguladora de las Haciendas Locales, añadiéndose un nuevo párrafo a dicho artículo, donde se establece que "Las Diputaciones Provinciales seguirán editando y publicando el Boletín Oficial de la Provincia, pudiendo a tal efecto establecer y exigir tasas y precios por la inserción de anuncios y edictos, y la suscripción y venta de ejemplares". Con este precepto se resolvió el problema económico planteado a las Diputaciones a la hora de hacer frente a los gastos ocasionados por la prestación de este servicio, si bien seguía sin existir una regulación específica del régimen jurídico de estos boletines.

Por su parte, el Congreso de los Diputados aprobó el 13 de diciembre de 2000 una Proposición no de Ley, en la que "insta al Gobierno a que, tras los oportunos estudios y consultas, se proceda a dictar la normativa adecuada del servicio de publicación del Boletín Oficial de la Provincia. Entre otros aspectos, esta nueva normativa preverá la posibilidad de que aquellas Comunidades Autónomas, en que así lo acuerden sus respectivos Parlamentos, puedan unificar en una sola publicación oficial los Boletines Oficiales de las Provincias de su territorio con el Boletín Oficial de la Comunidad Autónoma, de acuerdo con el respectivo Gobierno autonómico y los entes locales de su ámbito territorial".

En cumplimiento de este acuerdo, la presente Ley dota a los Boletines Oficiales de la Provincia de un marco jurídico completo y acorde con la actual configuración de la provincia en la Constitución Española de 1978 y en la propia Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, como entidad local dotada de autonomía para la gestión de sus respectivos intereses, previéndose expresamente la posibilidad de integración de estos boletines en el de la Comunidad Autónoma respectiva.

III

Así, se configura expresamente al Boletín Oficial de la Provincia como un servicio público de ámbito provincial, competencia de las Diputaciones Provinciales, a las que corresponde su edición y gestión. Al tratarse de una atribución competencial, es necesaria una norma con rango de Ley por imperativo del artículo 7.1 de la Ley 7/1985, de 2 de abril, donde se establece que las competencias propias de las entidades locales territoriales sólo podrán determinarse por Ley.

En este sentido, la necesidad de que las distintas Administraciones públicas y la propia Administración de Justicia dispongan de un instrumento para dar publicidad a sus disposiciones y actuaciones en el ámbito provincial queda atendida, estableciendo en la Ley la inserción obligatoria de aquéllas.

Por otra parte, como viene sucediendo en la actualidad, la publicación de los textos estará sujeta a la correspondiente ordenanza reguladora del servicio aprobada por la Diputación Provincial, de acuerdo con lo previsto en el artículo 122 de la Ley 39/1988, de 28 de diciembre, reguladora de las Haciendas Locales, siendo la suscripción obligatoria para los Entes locales de la provincia.

IV

En las disposiciones adicionales se contempla la posibilidad de que las Comunidades Autónomas puedan acordar la integración de los Boletines Oficiales de sus Provincias en el Boletín Oficial de la Comunidad, a fin de posibilitar una simplificación en los instrumentos de publicidad normativa existentes, si bien dicha posibilidad deberá contar con el acuerdo de la

Diputación Provincial, a fin de respetar los ámbitos de autonomía de la provincia y de la Comunidad Autónoma respectiva.

Por otro lado, también se contempla el reconocimiento de los regímenes especiales derivados de la Constitución y de los Estatutos de Autonomía recogidos en los artículos 39 a 41 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

V

Por último, la Ley se dicta al amparo de las competencias reconocidas al Estado en el artículo 149.1.18.a de la Constitución, por tratarse de una base del régimen jurídico administrativo que garantiza un tratamiento común a todos los ciudadanos, en relación con el artículo 9.3 de la Constitución (principio de publicidad de las normas), a lo que hay que añadir, en el presente caso, la relación existente con el principio de publicidad de las actuaciones judiciales, recogido en el artículo 120.1 de la Constitución.

En este sentido, el Tribunal Constitucional, en el fundamento jurídico 8 de la sentencia 233/1999, de 16 de diciembre, señala, por un lado, que la publicación de los actos jurídicos emanados de las Corporaciones Locales en los Boletines Oficiales de las Provincias ha de considerarse una decisión básica incardinable en la competencia atribuida al Estado por el artículo 149.1.18.a de la Constitución, pues exige un tratamiento común y uniforme en todo el territorio del Estado que sólo puede garantizar el legislador estatal, y, por otro lado, que la publicación de anuncios y acuerdos en el Boletín Oficial de la Provincia resulta plenamente acorde con la dimensión constitucional que a ésta atribuye el artículo 141 de la Constitución, en su doble condición de agrupación de municipios y división territorial para el cumplimiento de las actividades del Estado, entre las que hay que incluir las de las propias Corporaciones Locales en que se organiza territorialmente este último.

CAPÍTULO I

El Boletín Oficial de la Provincia

Artículo 1. *Contenido.*

El Boletín Oficial de la Provincia es el periódico oficial en el que se publicarán las disposiciones de carácter general y las ordenanzas, así como los actos, edictos, acuerdos, notificaciones, anuncios y demás resoluciones de las Administraciones públicas y de la Administración de Justicia de ámbito territorial provincial, cuando así esté previsto en disposición legal o reglamentaria.

Los textos publicados en el Boletín Oficial de la Provincia tienen la consideración de oficiales y auténticos.

Artículo 2. *Competencia.*

El Boletín Oficial de la Provincia es un servicio público de carácter provincial, competencia propia de las Diputaciones Provinciales, a las que corresponde su edición y gestión.

Cada Diputación Provincial regulará el modo y forma de gestión del Boletín, su edición, distribución y venta. A tal efecto, deberá aprobar la oportuna ordenanza reguladora del servicio, pudiendo a tal efecto establecer y exigir tasas y precios por la inserción de anuncios y edictos, y la suscripción y venta de ejemplares.

Artículo 3. *Suscripción.*

La suscripción al Boletín Oficial de la Provincia será obligatoria para los entes locales de la provincia, que deberán abonar la misma en los términos y con las excepciones que prevean las ordenanzas reguladoras.

Artículo 4. *Periodicidad.*

El Boletín Oficial de la Provincia se publicará con periodicidad mínima de tres veces por semana, debiendo coincidir la fecha del Boletín con la de su efectiva publicación.

Artículo 5. *Lengua de publicación.*

El Boletín Oficial de la Provincia se publicará en castellano y, en su caso, en la lengua que sea cooficial en el territorio, conforme a lo establecido por la legislación específica de las Comunidades Autónomas.

Artículo 6. *Obligación de publicar.*

1. Las Diputaciones Provinciales están obligadas a publicar en el Boletín Oficial de la Provincia cuantas disposiciones, ordenanzas, resoluciones, edictos, anuncios, actos o acuerdos de las distintas Administraciones públicas y de la Administración de Justicia deban ser insertados en el mismo en virtud de disposición legal o reglamentaria, así como otros actos o anuncios que aquéllas les remitan, sin perjuicio de lo establecido en el artículo 11 de esta Ley.

La orden de inserción corresponde al órgano competente de la correspondiente Administración anunciante, y será cumplimentada por la Diputación Provincial siempre que cumpla los requisitos establecidos en la presente Ley.

2. Los anuncios particulares podrán, asimismo, ser insertados en el Boletín Oficial de la Provincia, en los términos que se regulen en la correspondiente ordenanza provincial.

Artículo 7. *Publicación de los originales.*

1. Los originales serán transcritos en la misma forma en que se hallen redactados y autorizados por el órgano remitente, sin que por ninguna causa puedan variarse o modificarse sus textos una vez éstos hayan tenido entrada en el Boletín Oficial, salvo que el órgano remitente lo autorice de forma fehaciente.

2. La publicación de los originales se realizará por orden cronológico de presentación, que sólo podrá ser alterado cuando la publicación sea declarada urgente por el órgano remitente en la orden de inserción, o cuando el volumen del texto a publicar así lo exija, respetándose en todo caso el plazo máximo establecido en el apartado siguiente.

3. La publicación deberá ser realizada en el plazo máximo de 15 días hábiles posteriores al pago de la tasa correspondiente, si éste procediera, o, en su defecto, de la recepción de la orden de inserción. En caso de publicación urgente, dicho plazo se reducirá a 6 días hábiles.

4. Los originales que se envíen al Boletín Oficial de la Provincia tendrán carácter reservado. No podrá facilitarse información alguna acerca de los mismos, salvo autorización expresa del órgano remitente.

5. Si algún texto aparece publicado con erratas que alteren o modifiquen su contenido, será reproducido inmediatamente en su totalidad o en la parte necesaria, con las debidas correcciones.

Artículo 8. *Autentificación de documentos.*

A fin de comprobar la autenticidad de los documentos, los servicios correspondientes de la Diputación Provincial llevarán un registro de las autoridades y funcionarios facultados para firmar la orden de inserción de los originales destinados a su publicación, en el que constarán la firma autógrafa y el nombre y cargo de la persona a la que pertenezca.

A estos efectos, los órganos correspondientes de las Administraciones públicas y de la Administración de Justicia acreditarán ante la Diputación Provincial, según su normativa específica, a las personas facultadas para ordenar la inserción, así como las modificaciones que se produzcan.

Artículo 9. *Incorporación de medios técnicos.*

Conforme a lo dispuesto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las Diputaciones Provinciales impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos en la prestación del servicio del Boletín Oficial de la Provincia, debiendo quedar en todo caso garantizada la autenticidad de los documentos insertados.

Artículo 10. *Consulta del Boletín.*

Las Diputaciones Provinciales facilitarán en sus locales la consulta pública y gratuita del Boletín Oficial de la Provincia.

Esta obligación será extensiva a los Ayuntamientos de la provincia.

CAPÍTULO II

Régimen económico del Boletín Oficial de la Provincia

Artículo 11. *Tasa de publicación.*

1. La publicación de los textos en el Boletín Oficial de la Provincia estará sujeta al previo pago de la tasa provincial, de acuerdo con lo que establezca la ordenanza reguladora aprobada por la correspondiente Diputación Provincial.

2. Estarán exentos del pago de la tasa:

a) La publicación de disposiciones y las resoluciones de inserción obligatoria.

b) Los anuncios oficiales, cualquiera que sea el solicitante de la inserción, cuando la misma resulte obligatoria, de acuerdo con una norma legal o reglamentaria, así como los edictos y anuncios de Juzgados y Tribunales cuando la inserción sea ordenada de oficio.

3. Se exceptúan de la exención a que se refiere el apartado anterior las siguientes publicaciones:

a) Los anuncios publicados a instancia de particulares.

b) Los anuncios de licitaciones de todo tipo de contratos, de acuerdo con lo establecido en su legislación específica.

c) Los anuncios oficiales de la Administración de Justicia a instancia de particulares.

d) Los anuncios cuyo coste sea repercutible a los interesados según las disposiciones aplicables.

e) Los anuncios derivados de procedimientos sujetos al pago de una tasa, precio público u otro tipo de derechos económicos.

f) Los anuncios que puedan reportar, directa o indirectamente, un beneficio económico al remitente o solicitante, o tuvieran contenido económico.

No se considerará, a estos efectos, que reporta un beneficio económico o que tenga contenido económico las citaciones para ser notificados por comparecencia en los procedimientos de recaudación de los diferentes tributos o exacciones parafiscales, en los casos en que, intentada la notificación al interesado o representante por parte de la Administración tributaria o entidades y corporaciones de derecho público a las que corresponde su recaudación, ésta no haya sido posible.

g) Los anuncios que puedan o deban publicarse además en un diario, según disposición legal o reglamentaria.

La respectiva ordenanza reguladora de la tasa podrá declarar la exención de todos o alguno de los supuestos exceptuados.

Artículo 12. *Convenios de colaboración.*

Las ordenanzas reguladoras de las tasas podrán prever la posibilidad de suscripción de convenios de colaboración interadministrativa mediante los cuales se arbitren sistemas específicos para realizar la liquidación y pago global de las tasas por publicación de textos, en cuyo caso no será de aplicación lo previsto en el artículo anterior.

Con la misma finalidad, podrán suscribirse convenios para el pago de las tasas correspondientes a la publicación de anuncios particulares, en los términos que fijen las correspondientes ordenanzas.

Artículo 13. *Cooperación interadministrativa.*

De acuerdo con lo establecido en los artículos 55.d) de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, y 4.1.d) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo

Común, la Administración General del Estado y la de las Comunidades Autónomas prestarán, en el ámbito propio, la cooperación y asistencia activas que la Administración provincial pueda precisar para el mantenimiento y modernización del Boletín Oficial de la Provincia.

Disposición adicional primera. *Integración de los Boletines Oficiales de las Provincias.*

1. Los Parlamentos de las Comunidades Autónomas podrán, a propuesta del Gobierno autonómico, y previa aceptación de la Diputación Provincial, acordar la integración del Boletín Oficial de la Provincia en el Boletín Oficial de la Comunidad Autónoma respectiva, en cuyo caso se regulará por la normativa autonómica, siendo en todo caso de aplicación lo previsto en los artículos 1 ; 4 ; 5; 6, apartado 1; y 7, apartados 1, 4 y 5, de la presente Ley.

Asimismo, la referencia contenida en el artículo 6.1 a las Diputaciones Provinciales se entenderá realizada al órgano encargado de la publicación del Boletín Oficial de la respectiva Comunidad Autónoma, correspondiendo a ésta establecer el régimen económico de las citadas publicaciones.

2. En los casos en que se acuerde esta integración, el Boletín Oficial de cada una de las Provincias contará con una sección independiente identificada con su nombre o bien deberá señalarse claramente en el encabezamiento del Boletín Oficial de la Comunidad Autónoma respectiva que éste incluye los correspondientes Boletines Oficiales de las Provincias, a fin de garantizar la publicidad de sus contenidos.

3. El acuerdo de integración tendrá una vigencia de diez años, transcurridos los cuales se entenderá automáticamente prorrogado cada diez años si no hay denuncia expresa del acuerdo por el Gobierno autonómico o la Diputación Provincial.

Disposición adicional segunda. *Comunidades Autónomas uniprovinciales.*

Los Boletines Oficiales de las Comunidades Autónomas uniprovinciales se regirán por su legislación específica, siéndoles en todo caso de aplicación los artículos de la presente Ley citados en el número 1 de la disposición adicional primera.

La referencia contenida en el artículo 6.1 a las Diputaciones Provinciales, se entenderá realizada al órgano correspondiente encargado de la publicación del Boletín Oficial de la respectiva Comunidad Autónoma uniprovincial, correspondiendo a ésta establecer el régimen económico de las citadas publicaciones.

Disposición adicional tercera. *Comunidad Foral de Navarra.*

La presente Ley será de aplicación en la Comunidad Foral de Navarra en los términos establecidos en la disposición adicional primera de la Constitución y en la Ley Orgánica 13/1982, de 10 de agosto, de Reintegración y Amejoramiento del Régimen Foral de Navarra.

La referencia contenida en el artículo 6.1 a las Diputaciones Provinciales se entenderá realizada al órgano correspondiente encargado de la publicación del Boletín Oficial de la Comunidad Foral, correspondiendo a ésta establecer el régimen económico de la citada publicación.

Disposición adicional cuarta. *Comunidad Autónoma de Canarias.*

Los Boletines Oficiales de las Provincias de Las Palmas y de Santa Cruz de Tenerife se regirán por su normativa específica, de acuerdo con lo dispuesto en la disposición transitoria sexta de la Ley Orgánica 10/1982, de 10 de agosto, de Estatuto de Autonomía de Canarias, respecto a las Mancomunidades Provinciales Interinsulares, siéndoles en todo caso de aplicación lo dispuesto en la disposición adicional segunda respecto a las Comunidades Autónomas uniprovinciales.

Disposición adicional quinta. *Territorios Históricos.*

La presente Ley será de aplicación a los Boletines Oficiales de los Territorios Históricos del País Vasco de acuerdo con las especificidades derivadas de lo previsto en la disposición adicional primera de la Constitución, el Estatuto de Autonomía para el País Vasco y la

disposición adicional segunda de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

La referencia contenida en el artículo 6.1 a las Diputaciones Provinciales se entenderá realizada a las Diputaciones Forales, correspondiendo a éstas establecer el régimen económico de las citadas publicaciones.

Disposición adicional sexta. *Ciudades de Ceuta y Melilla.*

La presente Ley será de aplicación a los Boletines Oficiales de las Ciudades de Ceuta y Melilla, que deberán publicarse con una periodicidad mínima de dos veces por semana.

La referencia contenida en el artículo 6.1 a las Diputaciones Provinciales, se entenderá realizada al órgano correspondiente encargado de la publicación del Boletín Oficial de la Ciudad, correspondiendo a ésta establecer el régimen económico de las citadas publicaciones.

Disposición transitoria primera. *Adecuación de ordenanzas.*

Las Diputaciones Provinciales deberán adecuar sus ordenanzas a lo establecido en esta Ley en el plazo máximo de seis meses a partir del 1 de enero del ejercicio económico siguiente a su entrada en vigor.

Disposición transitoria segunda. *Entrada en vigor del artículo 5.*

El artículo 5 será de aplicación a los dos años de la entrada en vigor de la presente Ley.

Disposición derogatoria única.

Quedan derogadas las Reales Órdenes de 20 de abril de 1833, 26 de marzo de 1837, 5 de julio de 1837, 9 de octubre de 1838, 6 de abril de 1839, 4 de abril de 1840, 24 de mayo de 1846, 3 de septiembre de 1846, 21 de enero de 1849, 15 de julio de 1849, 8 de octubre de 1856, 1 de agosto de 1871, 9 de julio de 1872, 3 de noviembre de 1907 y 8 de agosto de 1915.

Quedan asimismo derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta Ley.

Disposición final única. *Título competencial.*

La presente Ley constituye legislación básica, dictada al amparo del artículo 149.1.18.a de la Constitución.

§ 32

Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado»

Ministerio de la Presidencia
«BOE» núm. 37, de 12 de febrero de 2008
Última modificación: 12 de mayo de 2021
Referencia: BOE-A-2008-2389

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, vino a consagrar la relación con las Administraciones públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones.

Con el criterio de que los diarios o boletines oficiales no han de quedar al margen de este nuevo marco general de relación, por vía electrónica, entre los poderes públicos y los ciudadanos, el artículo 11.1 de la citada ley prevé que dichas publicaciones, cuando se realicen en las sedes electrónicas correspondientes, tendrán los mismos efectos que los atribuidos a la edición impresa. Y, en referencia específica al «Boletín Oficial del Estado», la ley dispone que su publicación electrónica «tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables». Esta previsión está sometida a plazo: deberá tener efecto desde el día 1 de enero de 2009, según se determina en la disposición final segunda de la misma ley.

El objetivo principal de este real decreto es dar cumplimiento a ese mandato legal. Ahora bien, el texto de esta nueva norma se inspira en la convicción de que la edición electrónica del Boletín no constituye sólo un paso de alcance meramente tecnológico, que se adopta ante los imperativos de una renovación técnica irreversible. Responde, además, a la conciencia de que la difusión de las normas jurídicas a través de las nuevas redes electrónicas (y muy especialmente por la red «Internet») sitúa la publicación normativa en un plano de accesibilidad y propagación muy superior a todo lo hasta ahora conocido. De ahí la relevancia de conferir a los textos normativos así publicados el carácter oficial y auténtico que durante siglos ha tenido, en exclusiva, su impresión en papel. De esta idea central derivan los contenidos principales de este real decreto.

En primer lugar, se establece el carácter universal y gratuito del acceso a la edición electrónica, y los requerimientos de su aparición diaria en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado.

Se definen, en segundo término, los mecanismos, procesos y demás condiciones y garantías necesarias que aseguren la autenticidad, integridad e inalterabilidad de los contenidos del diario, especialmente a través de la firma electrónica, así como dispositivos para la verificación de tales mecanismos por los propios ciudadanos usuarios de las redes electrónicas.

Igualmente, resulta insoslayable dar cumplimiento eficaz al principio de igualdad consagrado en el artículo 4.b) de la ley, de manera que ningún ciudadano pueda sentirse discriminado por el hecho de no disponer de los medios electrónicos necesarios. Se establecen, para ello, puntos de acceso en oficinas públicas, modalidades varias de apoyo y asistencia a la búsqueda de documentos, así como, en todo caso, la posibilidad, al alcance de todo ciudadano, de obtener una copia impresa en papel de la edición electrónica del Boletín, tanto del ejemplar diario completo como de cada disposición, acto o anuncio en él publicado.

Hay que destacar también que el inicio de la edición electrónica del Boletín no supone la desaparición de la edición impresa, que se mantiene, con el mismo carácter oficial y auténtico, a efectos de conservación y permanencia del diario oficial, y también como medio de difusión en los supuestos en que no resulte posible la aparición de la edición electrónica.

El presente real decreto no se limita a dar carta de naturaleza a la edición electrónica del Boletín Oficial del Estado en nuestra realidad jurídica e institucional. Incorpora, además, parte del Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado, en cuanto se refiere a características, contenido, estructura y procedimiento de publicación, aspectos estos que, en sustancia, resultan aplicables a la edición electrónica, si bien convenientemente renovados en vista de la experiencia de su aplicación y adaptados al nuevo panorama técnico hoy dibujado. En aras de una mayor claridad normativa se ha preferido que la ordenación del diario oficial continúe siendo objeto de una sola norma, lo que supondrá la derogación del Real Decreto hasta ahora vigente.

Se habilita, en fin, al Ministro de la Presidencia para adoptar las medidas y disposiciones necesarias para la ejecución y cumplimiento de lo dispuesto en este real decreto.

En su virtud, a propuesta de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, con la aprobación de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de febrero de 2008,

D I S P O N G O :

CAPÍTULO I

Disposiciones generales

Artículo 1. *Definición.*

El «Boletín Oficial del Estado», diario oficial del Estado español, es el medio de publicación de las leyes, disposiciones y actos de inserción obligatoria.

Artículo 2. *Edición electrónica.*

1. El «Boletín Oficial del Estado» se publica en edición electrónica con arreglo a las condiciones que se establecen en este real decreto, así como en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, y en su normativa de desarrollo.

2. Además de la edición electrónica del «Boletín Oficial del Estado», existirá, obtenida de ésta, una edición impresa con idénticas características y contenido, con la finalidad y en las condiciones previstas en el artículo 13.

Artículo 3. *Carácter oficial y auténtico.*

1. El texto de las leyes, disposiciones y actos publicados en el «Boletín Oficial del Estado» tendrá la consideración de oficial y auténtico, con arreglo a las normas y condiciones que se establecen en este real decreto.

2. El texto de las normas emanadas de las comunidades autónomas que se publiquen en el «Boletín Oficial del Estado» tendrá el carácter que le atribuyan los respectivos Estatutos.

Artículo 4. *Características.*

1. El «Boletín Oficial del Estado» se publicará todos los días del año, salvo los domingos.

2. En la cabecera del ejemplar diario, de cada disposición, acto o anuncio y de cada una de sus páginas figurará:

a) El escudo de España.
b) La denominación «Boletín Oficial del Estado».
c) El número del ejemplar diario, que será correlativo desde el comienzo de cada año.
d) La fecha de publicación.
e) El número de página.

3. En todas y cada una de las páginas se incluirá la dirección de la sede electrónica y el respectivo código de verificación que permitan contrastar su autenticidad, así como acceder a su contenido, en los términos previstos en el artículo 14.4.
4. La fecha de publicación de las disposiciones, actos y anuncios será la que figure en la cabecera y en cada una de las páginas del ejemplar diario en que se inserten.
5. En cada número del diario oficial se incluirá el sumario de su contenido, con indicación del número correlativo que corresponde a cada disposición, acto o anuncio publicado en el mismo.
6. Todas las disposiciones, actos y anuncios abrirán página.

Artículo 5. *Competencias.*

1. Corresponde al Ministerio de la Presidencia, a través de la Secretaría General Técnica-Secretariado del Gobierno la ordenación y control de la publicación de las disposiciones y actos administrativos que deban insertarse en el «Boletín Oficial del Estado», velando especialmente por el orden de prioridad de las inserciones, la salvaguardia de las competencias de los distintos órganos de la Administración y el cumplimiento de los requisitos formales necesarios en cada caso. Podrá también decidir la publicación, en su caso, de números extraordinarios.
2. Corresponde a la Agencia Estatal Boletín Oficial del Estado la edición, publicación y difusión del diario oficial «Boletín Oficial del Estado».

CAPÍTULO II

Contenido del «Boletín Oficial del Estado»

Artículo 6. *Contenido.*

1. En el «Boletín Oficial del Estado» se publicarán:

a) Las disposiciones generales de los órganos del Estado y los tratados o convenios internacionales.
b) Las disposiciones generales de las comunidades autónomas, de acuerdo con lo establecido en los Estatutos de Autonomía y en las normas con rango de ley dictadas para el desarrollo de los mismos.
c) Las resoluciones y actos de los órganos constitucionales del Estado, de acuerdo con lo establecido en sus respectivas leyes orgánicas.
d) Las disposiciones que no sean de carácter general, las resoluciones y actos de los departamentos ministeriales y de otros órganos del Estado y Administraciones públicas, cuando una ley o un real decreto así lo establezcan.
e) Las convocatorias, citaciones, requisitorias y anuncios cuando una ley o un real decreto así lo establezcan.

2. El Consejo de Ministros podrá excepcionalmente acordar la publicación de informes, documentos o comunicaciones oficiales, cuya difusión sea considerada de interés general.

Artículo 7. *Estructura del diario oficial.*

1. El contenido del "Boletín Oficial del Estado" se distribuye en las siguientes secciones:

Sección I: Disposiciones generales.
Sección II: Autoridades y personal.
Sección III: Otras disposiciones.

Sección IV: Administración de Justicia.
Sección V: Anuncios.
Sección del Tribunal Constitucional.

2. Existirán asimismo los siguientes suplementos de carácter independiente:

a) El Suplemento de notificaciones.
b) El Suplemento del Tablón Edictal Judicial Único.

Artículo 8. *Contenido de las secciones y suplementos.*

1. Se incluirán en la sección I:

a) Las leyes orgánicas, las leyes, los reales decretos legislativos y los reales decretos-leyes.
b) Los tratados y convenios internacionales.
c) Las leyes de las asambleas legislativas de las comunidades autónomas.
d) Los reglamentos y demás disposiciones de carácter general.
e) Los reglamentos normativos emanados de los consejos de gobierno de las comunidades autónomas.

2. La sección II estará integrada por dos subsecciones:

a) Nombramientos, situaciones e incidencias.
b) Oposiciones y concursos.

3. La sección III estará integrada por las disposiciones de obligada publicación que no tengan carácter general ni correspondan a las demás secciones.
4. En la sección IV se publicarán:

a) Los anuncios de subastas judiciales.
b) Los actos procesales que no deban ser objeto de inserción en el Suplemento del Tablón Edictal Judicial Único, conforme a lo previsto en el párrafo primero del artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
5. En la sección V se insertarán los anuncios, salvo los de notificación, agrupados de la siguiente forma:

a) Contratación del Sector Público.
b) Otros anuncios oficiales.
c) Anuncios particulares.

6. En la sección del Tribunal Constitucional se publicarán las sentencias, declaraciones y autos del Tribunal Constitucional, en los términos previstos en su ley orgánica.
7. En el Suplemento de notificaciones se insertarán los anuncios de notificación.
8. El Suplemento del Tablón Edictal Judicial Único incluirá las resoluciones y comunicaciones de los Juzgados y Tribunales a las que se refiere el párrafo primero del artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
Este suplemento estará integrado por dos secciones:

a) Edictos judiciales de carácter general.
b) Edictos judiciales de carácter particular.

Artículo 9. *Estructura de las secciones y subsecciones.*

1. Dentro de cada sección, la inserción de los textos se realizará agrupándolos por el órgano del que procedan, según la ordenación general de precedencias del Estado. Las disposiciones emanadas de las comunidades autónomas se insertarán según el orden de publicación oficial de los Estatutos de Autonomía.
2. Dentro de cada epígrafe, los textos se ordenarán según la jerarquía de las normas.

CAPÍTULO III

Edición electrónica

Artículo 10. *Publicación de la edición electrónica.*

1. La edición electrónica del «Boletín Oficial del Estado» se publicará en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado.

2. La edición electrónica del «Boletín Oficial del Estado» respetará los principios de accesibilidad y usabilidad, de acuerdo con las normas establecidas al respecto, utilizará estándares abiertos y en su caso aquellos otros que sean de uso generalizado por los ciudadanos.

3. La sede electrónica de la Agencia Estatal Boletín Oficial del Estado se dotará de las medidas de seguridad que garanticen la autenticidad e integridad de los contenidos del diario oficial, así como el acceso permanente al mismo, con sujeción a los requisitos establecidos en el Esquema Nacional de Seguridad previsto en el artículo 42 de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos.

Artículo 11. *Acceso a la edición electrónica.*

1. La Agencia Estatal Boletín Oficial del Estado garantizará, a través de redes abiertas de telecomunicación, el acceso universal y gratuito a la edición electrónica del diario oficial del Estado, sin perjuicio de lo previsto en el artículo 14.4.

2. La edición electrónica del «Boletín Oficial del Estado» deberá estar accesible en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado en la fecha que figure en la cabecera del ejemplar diario, salvo que ello resulte imposible por circunstancias extraordinarias de carácter técnico.

Artículo 12. *Requisitos de la edición electrónica.*

1. La edición electrónica del «Boletín Oficial del Estado» deberá incorporar firma electrónica avanzada como garantía de la autenticidad, integridad e inalterabilidad de su contenido. Los ciudadanos podrán verificar el cumplimiento de estas exigencias mediante aplicaciones estándar o, en su caso, mediante las herramientas informáticas que proporcione la sede electrónica de la Agencia Estatal Boletín Oficial del Estado.

2. Corresponde a la Agencia Estatal Boletín Oficial del Estado:

a) garantizar la autenticidad, integridad e inalterabilidad del diario oficial que se publique en su sede electrónica.

b) custodiar y conservar la edición electrónica del diario oficial del Estado

c) velar por la accesibilidad de la edición electrónica del diario oficial del Estado y su permanente adaptación al progreso tecnológico.

3. La Agencia Estatal Boletín Oficial del Estado publicará en su sede electrónica las prácticas y procedimientos necesarios para la efectividad de lo previsto en este artículo.

Artículo 13. *Garantía de la edición.*

1. La edición impresa del diario oficial tiene las siguientes finalidades:

a) asegurar la publicación del «Boletín Oficial del Estado» cuando por una situación extraordinaria y por motivos de carácter técnico no resulte posible acceder a su edición electrónica;

b) garantizar la conservación y permanencia del diario oficial del Estado y su continuidad como parte del patrimonio documental impreso de la Administración General del Estado.

2. La edición impresa comprenderá los ejemplares necesarios para asegurar la conservación y custodia de al menos tres ejemplares del diario oficial en la Agencia Estatal Boletín Oficial del Estado y en la Secretaría General Técnica-Secretariado del Gobierno, así como los que reglamentariamente se determine para su conservación en la normativa que regula el depósito legal.

3. Los ejemplares de la edición impresa del diario oficial a los que se refiere el apartado anterior, serán realizados, conservados y custodiados de manera que quede garantizada su perdurabilidad.

4. No obstante lo dispuesto en los apartados anteriores, los suplementos de notificaciones y del Tablón Edictal Judicial Único solamente contarán con edición impresa cuando concurran las circunstancias previstas en la letra a) del apartado primero.

CAPÍTULO IV

Acceso de los ciudadanos al «Boletín Oficial del Estado»

Artículo 14. *Acceso de los ciudadanos.*

1. Los ciudadanos tendrán acceso libre y gratuito a la edición electrónica del «Boletín Oficial del Estado». Dicho acceso comprenderá la posibilidad de búsqueda y consulta del contenido del diario, así como la posibilidad de archivo e impresión, tanto del diario completo como de cada una de las disposiciones, actos o anuncios que lo componen.

2. En todas las oficinas de información y atención al ciudadano de la Administración General del Estado, se facilitará la consulta pública y gratuita de la edición electrónica del «Boletín Oficial del Estado. Con ese fin, en cada una de estas oficinas existirá al menos un terminal informático, a través del cual se podrán realizar búsquedas y consultas del contenido del diario. Las mencionadas oficinas deberán facilitar a las personas que lo soliciten una copia impresa de las disposiciones, actos o anuncios que requieran, o del diario completo, mediante, en su caso, la contraprestación que proceda.

3. Mediante orden del Ministro de la Presidencia podrán establecerse las condiciones de obtención de copias auténticas impresas de las disposiciones, actos o anuncios o del diario completo, tanto en la Agencia Estatal Boletín Oficial del Estado, como en las oficinas públicas de consulta.

4. No obstante lo previsto en los apartados anteriores, los suplementos permanecerán libremente accesibles en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado durante un plazo de tres meses, en el caso del Suplemento de notificaciones, y de cuatro meses, en el caso del Suplemento del Tablón Edictal Judicial Único.

Una vez transcurrido el plazo correspondiente a cada suplemento, el acceso requerirá el código de verificación del correspondiente documento, que tendrá carácter único y no previsible.

La conservación, almacenamiento y tratamiento de la información publicada en los suplementos solamente le está permitida a los interesados o a sus representantes, a los Juzgados y Tribunales, al Ministerio Fiscal, así como a las Administraciones que puedan precisarlo para el ejercicio de las competencias que les corresponden.

La Agencia Estatal Boletín Oficial del Estado adoptará medidas orientadas a evitar la indexación y recuperación automática de la información publicada en lo suplementos por parte de sujetos distintos a los contemplados en el párrafo anterior.

Sin perjuicio de lo previsto en las disposiciones adicionales primera y cuarta, finalizados los plazos previstos, respectivamente, en el párrafo primero de este apartado, la Agencia Estatal Boletín Oficial del Estado facilitará el documento publicado, previa solicitud, únicamente a los interesados o a sus representantes, al Ministerio Fiscal, al Defensor del Pueblo, y a los Juzgados y Tribunales.

Artículo 15. *Servicio de ayuda.*

La Agencia Estatal Boletín Oficial del Estado ofrecerá un servicio gratuito de asistencia a los ciudadanos en la búsqueda de las disposiciones, actos y anuncios publicados en el diario oficial y les facilitará, cuando así lo soliciten, una copia impresa de aquéllas, o del diario completo, mediante la correspondiente contraprestación que reglamentariamente se establezca.

Se exceptúan de lo previsto en el párrafo anterior los documentos publicados en los suplementos de notificaciones y del Tablón Edictal Judicial Único, una vez hayan transcurrido los plazos previstos, respectivamente, en el apartado cuatro del artículo 14.

Artículo 16. *Convenios con otras Administraciones públicas.*

Se celebrarán convenios con las comunidades autónomas, las administraciones locales, las universidades y otros entes públicos para que ofrezcan los servicios a los que se refieren los artículos 14 y 15.

Artículo 17. *Servicio de base de datos.*

La Agencia Estatal Boletín Oficial del Estado ofrecerá en su sede electrónica, con carácter diferenciado a la edición electrónica del ''Boletín Oficial del Estado'', una base de datos gratuita que permita la búsqueda, recuperación e impresión de las disposiciones, actos y anuncios publicados en el ''Boletín Oficial del Estado'', con sujeción a lo establecido en la normativa de protección de datos personales.

No obstante, la búsqueda, recuperación e impresión, a través del servicio de base de datos, de los documentos publicados en los suplementos de notificaciones y del Tablón Edictal Judicial Único, será posible exclusivamente durante los plazos previstos, respectivamente, en el apartado cuatro del artículo 14.

Artículo 18. *Accesibilidad.*

La edición electrónica del diario oficial tendrá las condiciones de accesibilidad necesarias para su consulta por las personas con discapacidad o de edad avanzada.

CAPÍTULO V

Procedimiento de publicación

Artículo 19. *Facultad de ordenar la inserción.*

1. La inserción en el diario oficial del Estado de las leyes aprobadas por las Cortes Generales se hará del modo previsto en el artículo 91 de la Constitución.

2. La facultad de ordenar la inserción de los reales decretos-leyes corresponde al Ministro que ejerza la secretaría del Consejo de Ministros. La de los reales decretos legislativos y los reales decretos, al ministro que los refrende o, por su delegación, a los demás órganos superiores del departamento correspondiente.

3. La facultad de ordenar la inserción de las restantes disposiciones y actos queda atribuida del siguiente modo:

a) En los departamentos ministeriales, a los Ministros, Secretarios de Estado en el ámbito de su competencia, Subsecretarios, Secretarios Generales Técnicos y los Directores Generales o equivalentes. Cuando se trate de normas o actos dictados a propuesta de varios departamentos, la publicación será ordenada por los correspondientes órganos del Ministerio de la Presidencia.

b) Las disposiciones y actos emanados de los órganos constitucionales del Estado y de otras Administraciones Públicas, a las autoridades que tengan atribuida la representación de cada órgano o Administración o a aquellos en los que se delegue expresamente.

4. La facultad de ordenar la inserción de los anuncios u otros actos que deban publicarse en las Secciones IV y V del Boletín Oficial del Estado, la tendrán las autoridades que en los órganos constitucionales del Estado o en cada Administración o entidad tengan atribuida la competencia o estén autorizados para ello.

5. La facultad de ordenar la inserción de los anuncios de notificación que deban publicarse en el Suplemento de notificaciones corresponde a los órganos que en cada Administración o entidad, tengan atribuida dicha competencia o estén autorizados para ello, así como a los órganos que hayan emitido los correspondientes anuncios.

6. La facultad de ordenar la inserción de los actos procesales que deban publicarse en el Suplemento del Tablón Edictal Judicial Único corresponde a los Juzgados y Tribunales en los términos previstos por las normas procesales.

Artículo 20. *Remisión de documentos.*

1. Los originales destinados a la publicación en las secciones I, II, III y del Tribunal Constitucional se remitirán en formato electrónico, de acuerdo con las garantías, especificaciones y modelos que para cada órgano y Administración se establezcan mediante orden del Ministro de la Presidencia y que figuren en las sedes electrónicas del Ministerio de la Presidencia y de la Agencia Estatal Boletín Oficial del Estado.

2. Los originales destinados a la publicación en las secciones IV y V se remitirán en formato electrónico, de acuerdo con las garantías, especificaciones y modelos que se establezcan mediante resolución de la Agencia Estatal Boletín Oficial del Estado, publicada en su sede electrónica.

3. Los originales destinados a la publicación en el Suplemento de notificaciones se remitirán mediante el sistema automatizado de remisión y gestión telemática previsto en la disposición adicional tercera de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, de acuerdo con las garantías, especificaciones básicas y modelos que se establecen en la disposición adicional primera de este real decreto.

4. Los originales destinados a la publicación en el Suplemento del Tablón Edictal Judicial Único se remitirán mediante el sistema automatizado de remisión y gestión telemática previsto en el artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, de acuerdo con las garantías, especificaciones básicas y modelos que se establecen en la disposición adicional cuarta de este real decreto.

5. En todo caso, el formato de los documentos, ya sea de texto, gráfico, de imagen o cualquier otro, deberá atender los estándares que garanticen el adecuado nivel de interoperabilidad y resultar idóneo para comunicar el contenido del documento de que se trate.

Artículo 21. *Autenticidad de los documentos.*

1. Respecto a las disposiciones y actos de las secciones I, II, III y del Tribunal Constitucional, se aplicarán las siguientes normas:

a) La autenticidad de los originales remitidos para publicación habrá de quedar garantizada mediante su firma electrónica, de conformidad con lo que prevea la orden del Ministro de la Presidencia a la que se refiere el artículo 20.

b) A tal efecto, en la Secretaría General Técnica-Secretariado del Gobierno existirán los registros de firmas electrónicas de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

c) En cada departamento ministerial, el Subsecretario determinará las tres autoridades o funcionarios que, además de los titulares de los órganos superiores, estarán facultados para firmar la inserción de los originales destinados a publicación.

d) Los órganos constitucionales y las Administraciones públicas, de acuerdo con su normativa específica, determinarán las autoridades o funcionarios facultados para firmar la inserción de originales, sin que el número de firmas reconocidas pueda exceder de tres por cada órgano o Administración.

e) La autoridad o funcionario que suscriba la inserción de los originales se hará responsable de la autenticidad de su contenido y de la existencia de la correspondiente orden de inserción adoptada en los términos a los que se refiere el artículo 19.

2. Respecto a los anuncios y otros actos de las secciones IV y V, la Agencia Estatal Boletín Oficial del Estado mantendrá un registro de las entidades y organismos firmantes de los anuncios que se publiquen en el diario oficial. La autenticidad de los originales remitidos para publicación deberá quedar garantizada mediante alguno de los sistemas de firma electrónica previstos en el artículo 13 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

3. Respecto de los anuncios de notificación que se publiquen en el Suplemento de notificaciones, la autenticidad de los originales remitidos para publicación deberá quedar garantizada en los términos previstos en la disposición adicional primera.

4. Respecto de los documentos que se publiquen en el Suplemento del Tablón Edictal Judicial Único, la autenticidad de los originales remitidos para publicación deberá quedar garantizada en los términos previstos en la disposición adicional cuarta.

Artículo 22. *Competencia en relación con las diversas secciones.*

1. Los textos de las disposiciones, resoluciones, sentencias y actos incluidos en las secciones I, II, III y del Tribunal Constitucional serán remitidos, en todo caso, a la Secretaría General Técnica-Secretariado del Gobierno, que procederá a la clasificación de los mismos y a la comprobación de la autenticidad de las firmas, velando especialmente por el orden de prioridad de las inserciones, la salvaguarda de las competencias de los distintos órganos de la Administración, la obligatoriedad de la inserción y el cumplimiento de los requisitos formales necesarios en cada caso.

2. Los originales de los anuncios y otros actos que deban insertarse en las secciones IV y V se remitirán directamente por los organismos, entidades y personas interesadas a la Agencia Estatal Boletín Oficial del Estado o, en su caso, a través de la Plataforma de Contratación del Sector Público.

3. Los anuncios de notificación se remitirán a la Agencia Estatal Boletín Oficial del Estado, en los términos previstos en las disposiciones adicionales primera y segunda.

4. Los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único, se remitirán a la Agencia Estatal Boletín Oficial del Estado en los términos previstos en la disposición adicional cuarta.

Artículo 23. *Tramitación de la documentación.*

1. Los originales recibidos para publicación en el «Boletín Oficial del Estado» tendrán carácter reservado y no podrá facilitarse información acerca de ellos.

2. Los originales serán insertados en los mismos términos en que se hallen redactados y autorizados, sin que puedan modificarse, salvo autorización del organismo remitente.

Artículo 24. *Publicación íntegra y en extracto.*

1. Las disposiciones, resoluciones, sentencias y actos incluidos en la sección I y en la sección del Tribunal Constitucional se publicarán en forma íntegra.

2. Las resoluciones y actos comprendidos en las secciones II, III, IV y V, así como en el Suplemento de notificaciones, se publicarán en extracto, siempre que sea posible y se reúnan los requisitos exigidos en cada caso.

Los actos procesales objeto de inserción en el Suplemento del Tablón Edictal Judicial Único se publicarán en extracto, en los términos establecidos por las normas procesales. En todo caso, deberán quedar salvaguardados los derechos e intereses de los menores, así como otros derechos y libertades que pudieran verse afectados por la publicación.

3. Los organismos remitentes enviarán debidamente extractados los textos y documentos susceptibles de ser publicados en esta forma.

Artículo 25. *Justificación de la obligatoriedad de la inserción.*

Cuando se susciten dudas sobre la procedencia de publicar una determinada disposición o texto, el organismo remitente hará constar en su escrito la norma en la que se establezca la obligatoriedad de la inserción.

Artículo 26. *Correcciones.*

Si alguna disposición oficial aparece publicada con errores que alteren o modifiquen su contenido, será reproducida inmediatamente en su totalidad o en la parte necesaria, con las debidas correcciones. Estas rectificaciones se realizarán de acuerdo con las siguientes normas:

a) Se corregirán de oficio las erratas padecidas en la publicación, siempre que supongan alteración o modificación del sentido de las mismas o puedan suscitar dudas al respecto. A tal efecto, los correspondientes servicios de la Secretaría General Técnica-Secretariado del

Gobierno y de la Agencia Estatal Boletín Oficial del Estado, conservarán los originales de cada número, durante el plazo de tres meses, a partir de la fecha de su publicación.

b) Cuando se trate de errores padecidos en el texto recibido en la Agencia Estatal Boletín Oficial del Estado para publicación, su rectificación se realizará del modo siguiente:

1.º Los meros errores u omisiones materiales, que no constituyan modificación o alteración del sentido de las disposiciones o se deduzcan claramente del contexto, pero cuya rectificación se juzgue conveniente para evitar posibles confusiones, se salvarán por los organismos respectivos instando la reproducción del texto, o de la parte necesaria del mismo, con las debidas correcciones.

2.º En los demás casos, y siempre que los errores u omisiones puedan suponer una real o aparente modificación del contenido o del sentido de la norma, se salvarán mediante disposición del mismo rango.

Artículo 27. *Inserciones gratuitas y de pago.*

1. La publicación de las leyes, disposiciones, resoluciones, sentencias y actos de inserción obligatoria que deban ser incluidos en las secciones I, II, III y del Tribunal Constitucional, se efectuará sin contraprestación económica por parte de los órganos que la hayan interesado.

2. La publicación de anuncios en las secciones IV y V está sujeta al pago de la correspondiente tasa, de acuerdo con lo dispuesto en la Ley 25/1998, de 13 de julio, de modificación del régimen legal de las tasas estatales y de reordenación de las prestaciones patrimoniales de carácter público y en el Estatuto de la Agencia Estatal Boletín Oficial del Estado, aprobado por Real Decreto 1495/2007, de 12 de noviembre.

3. La publicación de documentos en los suplementos de notificaciones y del Tablón Edictal Judicial Único se efectuará sin contraprestación económica alguna por parte de los organismos que la hayan interesado.

Disposición adicional primera. *Sistema automatizado de remisión y gestión telemática de los anuncios de notificación.*

1. El sistema automatizado de remisión y gestión telemática de la Agencia Estatal Boletín Oficial del Estado, para la publicación de los anuncios de notificación, previsto en la disposición adicional vigésima primera de la Ley 30/1992, de 26 de noviembre, deberá ajustarse a las siguientes garantías y especificaciones básicas:

a) El acceso al sistema requerirá previa identificación, que podrá realizarse mediante DNI electrónico o certificado electrónico reconocido. Asimismo, podrá requerirse estar dado de alta en el repositorio horizontal de usuarios de las Administraciones Públicas. En caso de que el acceso se realice mediante servicios web, se podrá utilizar el sistema de firma electrónica mediante sello electrónico del correspondiente órgano, entidad o Administración.

Cada Administración Pública o entidad determinará, de acuerdo con su normativa específica, las autoridades o empleados públicos autorizados. En el caso de las entidades locales, la autorización inicial deberá ser comunicada telemáticamente a la Agencia Estatal Boletín Oficial del Estado por un funcionario de Administración local con habilitación de carácter nacional.

b) Las Administraciones y entidades usuarias estarán obligadas a mantener permanentemente actualizado el catálogo de unidades administrativas implicadas en el procedimiento de publicación, mediante el directorio común a que se refiere el artículo 9 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.

c) La remisión se realizará preferentemente mediante servicios web conforme al formato estructurado que se contiene en el anexo de este real decreto, el cual podrá ser actualizado mediante resolución de la Agencia Estatal Boletín Oficial del Estado. Asimismo, la remisión podrá realizarse por medio de un portal web. En todo caso, deberán incorporarse los metadatos que permitan la gestión automatizada de los documentos por parte de la Agencia Estatal Boletín Oficial del Estado.

d) El sistema de remisión garantizará la autenticidad, integridad y no repudio de los envíos, así como su confidencialidad.

e) El sistema permitirá consultar, mediante servicios web u otros mecanismos, el estado de tramitación de los anuncios de notificación enviados, así como acceder a su publicación sin limitación temporal alguna, en los términos que cada Administración Pública o entidad haya autorizado, conforme a lo previsto en la letra a) de este apartado.

f) Los anuncios de notificación serán publicados dentro de los tres días hábiles siguientes a su recepción, salvo los supuestos de imposibilidad técnica, solicitud de un plazo de publicación superior por el órgano remitente o que el anuncio de notificación requiera de subsanación. A estos efectos, los anuncios de notificación recibidos después de las 12:00 horas del viernes, los sábados, días festivos y 24 y 31 de diciembre se considerarán recibidos a las 8:00 horas del primer día hábil siguiente.

2. Corresponde a la Agencia Estatal Boletín Oficial del Estado determinar los requisitos y las especificaciones técnicas del sistema, que, en todo caso, deberá cumplir con lo establecido en la Ley 11/2007, de 22 de junio, y su normativa de desarrollo.

Disposición adicional segunda. *Anuncios de notificación en procedimientos sancionadores en materia de tráfico.*

(Derogada)

Téngase en cuenta que esta disposición se deroga con efectos de 1 de enero de 2022, según establece la disposición derogatoria única del Real Decreto 327/2021, de 11 de mayo. Ref. BOE-A-2021-7843

Redacción anterior:

"Sin perjuicio de lo previsto en la disposición adicional primera, los anuncios de notificación a que dé lugar el procedimiento sancionador como consecuencia de la comisión de infracciones a la normativa sobre tráfico, circulación de vehículos a motor y seguridad vial, podrán remitirse a la Agencia Estatal Boletín Oficial del Estado a través de la Dirección General de Tráfico."

Disposición adicional tercera. *Remisión telemática de documentos a publicar en las secciones I, II, III y del Tribunal Constitucional.*

Las garantías, especificaciones y modelos a los que se refiere el artículo 20.1 son los previstos en las Ordenes PRE/1563/2006, de 19 de mayo, por la que se regula el procedimiento para la remisión telemática de las disposiciones y actos administrativos de los departamentos ministeriales que deban publicarse en el "Boletín Oficial del Estado" y PRE/987/2008, de 8 de abril, por la que se amplía su ámbito de aplicación, para los departamentos ministeriales, órganos y entidades previstos en sus respectivos ámbitos de aplicación.

Disposición adicional cuarta. *Sistema automatizado de remisión y gestión telemática de los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único.*

1. El sistema automatizado de remisión y gestión telemática de la Agencia Estatal Boletín Oficial del Estado, previsto en el artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, se ajustará a las siguientes garantías y especificaciones básicas:

a) El acceso al sistema requerirá previa identificación de los funcionarios al servicio del órgano judicial competente, que podrá realizarse mediante DNI electrónico u otro certificado electrónico cualificado. En caso de que el acceso se realice mediante servicios web, se deberá utilizar el sistema de firma electrónica mediante sello electrónico cualificado del correspondiente sistema de gestión procesal.

b) El Ministerio de Justicia mantendrá permanentemente actualizado y accesible mediante servicios web, el catálogo de órganos judiciales y de usuarios implicados en el

procedimiento de publicación y el Ministerio de Defensa, respecto de los órganos judiciales militares.

c) La remisión se realizará preferentemente mediante servicios web conforme al formato estructurado que se contiene en el anexo II de este real decreto. Asimismo, la remisión podrá realizarse por medio de un portal web. En todo caso, deberán incorporarse los metadatos que permitan la gestión automatizada de los documentos por parte de la Agencia Estatal Boletín Oficial del Estado.

d) El sistema de remisión garantizará la autenticidad, integridad y no repudio de los envíos, así como su confidencialidad.

e) El sistema permitirá consultar, mediante servicios web u otros mecanismos, el estado de tramitación de los documentos enviados, así como acceder a su publicación sin limitación temporal alguna, conforme a lo previsto en la letra a) de este apartado.

f) Los documentos serán publicados dentro de los tres días hábiles siguientes a su recepción, salvo los supuestos de imposibilidad técnica, solicitud de un plazo de publicación superior por el remitente o que el documento requiera de subsanación. A estos efectos, los documentos recibidos después de las 12:00 horas del viernes, los sábados, días festivos y 24 y 31 de diciembre se considerarán recibidos a las 8:00 horas del primer día hábil siguiente.

2. Corresponde a la Dirección de la Agencia Estatal Boletín Oficial del Estado determinar los requisitos y las especificaciones técnicas del sistema.

Disposición transitoria única. *Remisión de documentos a publicar en las secciones I, II, III y del Tribunal Constitucional.*

En tanto no se aprueben las garantías, especificaciones y modelos para los órganos y Administraciones no contemplados en el ámbito de aplicación de las Órdenes PRE/1563/2006, de 19 de mayo, y PRE/987/2008, de 8 de abril, continuarán remitiéndose los originales a publicar en formato papel, con firma manuscrita de quien esté facultado al efecto, acompañados de los ficheros electrónicos a partir de los cuales se generaron los originales remitidos y ajustándose en todas sus características a los modelos oficiales que figuran en las sedes electrónicas del Ministerio de la Presidencia y de la Agencia Estatal Boletín Oficial del Estado.

A estos efectos, la Secretaría General Técnica-Secretariado del Gobierno mantendrá un registro de firmas manuscritas de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogado el Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado.

2. Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Habilitación normativa.*

1. Se autoriza al Ministro de la Presidencia para que dicte cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en este real decreto, y en particular para el establecimiento de las garantías y especificaciones con arreglo a las cuales los originales destinados a la publicación en el «Boletín Oficial del Estado» podrán remitirse a través de medios electrónicos, informáticos y telemáticos, así como para el establecimiento de los modelos electrónicos que deban emplearse para la remisión telemática de los originales de disposiciones o actos que deban ser insertados en el «Boletín Oficial del Estado».

2. Los anexos I y II podrán ser actualizados mediante resolución de la Dirección de la Agencia Estatal Boletín Oficial del Estado, que deberá publicarse en el “Boletín Oficial del Estado”.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día 1 de enero de 2009.

ANEXO I

Formato XML para el envío de anuncios de notificación

El contenido del envío se realizará en formato XML con la información estructurada de la siguiente forma:

```
<envio>
    <version>
    <anuncios>
        <remitente>
            <nodoRemitente +>
        </remitente>
        <fechaPub ?>
        <infPub>
            <urlSW ?>
            <email>
        </infPub>
        <anuncio +>
            <emisor>
                <nodoEmisor +>
            </emisor>
            <metadatos>
                <id ?>
                <formPub>
                <datosPersonales>
                <lgt ?>
                <procedimiento ?>
                <materias ?>
                    <materia +>
                </materias>
                <notificados ?>
                    <notificado +>
                </notificados>
            </metadatos>
            <contenido>
                <texto>
                    <p +>
                    <table *>
                </texto>
                <pieFirma>
                    <lugar>
                    <fecha>
                    <firmante>
                </pieFirma>
            </contenido>
            <contenidoCoof ?>
                <texto>
                    <p +>
                    <table *>
                </texto>
            </contenidoCoof>
        </anuncio>
    </anuncios>
</envio>

+ significa una o más ocurrencias
? significa cero o una ocurrencia
* significa cero o más ocurrencias
```

En la descripción de los contenidos del fichero XML se hace referencia a una serie de tipos de datos por su acrónimo. A continuación se enumeran estos tipos de datos.

NIF: Número de Identificación Fiscal. Deberá proporcionarse siempre justificado con «0» a la izquierda, sin puntos, ni espacios, ni guiones ni ningún otro carácter distinto de un número o una letra.

NAF: Número de afiliación a la Seguridad Social.

CCC: Código de cuenta de cotización.

EXP: Número de expediente.

DIR3: Directorio común de Unidades orgánicas y oficinas. La descripción de este servicio se encuentra en el PAE (portal de administración electrónica) en la siguiente URL: http://administracionelectronica.gob.es/ctt/dir3.

La Agencia Estatal Boletín Oficial del Estado pondrá asimismo en su sede electrónica el fichero XSD (XML Schema Definition) para la validación previa al envío de los ficheros XML con el contenido de los anuncios, la documentación del servicio web para el envío de dichos ficheros y ejemplos de ficheros XML con distintos tipos de notificaciones.

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
	envio	Nodo raíz del envío		[1..1]	
1	version	Código que indica la versión utilizada. Existirá compatibilidad de versiones.	[1.0.0]	[1..1]	string
2	anuncios			[1..1]	complexType
2.1	remitente	Organismo o unidad remitente de los anuncios. Contiene el árbol de la estructura del directorio DIR3 del organismo o unidad, incluyendo un elemento nodoRemitente para cada nivel en DIR3.		[1..1]	complexType
2.1.1	nodoRemitente	Organismo o unidad remitente de los anuncios. Contiene dos atributos: idDir3: Código DIR3 del organismo. Tipo dato: string. nivel: Nivel dentro del árbol conforme a la estructura DIR3. Tipo dato: int. Por ejemplo, en el caso de la Agencia Estatal Boletín Oficial del Estado sería: <nodoRemitente nivel="1" idDir3="EA9999999">ADMINISTRACIÓN GENERAL DEL ESTADO</nodoRemitente> <nodoRemitente nivel="2" idDir3="E00004101">MINISTERIO DE LA PRESIDENCIA</nodoRemitente> <nodoRemitente nivel="3" idDir3="E00135501">SUBSECRETARIA DE LA PRESIDENCIA</nodoRemitente> <nodoRemitente nivel="4" idDir3="E04761001">AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO</nodoRemitente>		[1..*]	string
2.2	fechaPub	Fecha de publicación solicitada para los anuncios. Si la fecha se correspondiese con un domingo, la publicación se realizará el lunes siguiente. Si no se incluye o es incorrecta se procederá a publicar en la fecha más temprana posible conforme al procedimiento de cierre y publicación que rige la publicación del BOE. La fecha se especificará en formato ISO 8601:2004 (aaaa-mm-dd). Por ejemplo: <fechaPub>2015-11-01</fechaPub> Nota: El BOE se publica todos los días del año con la única excepción de los domingos.		[0..1]	date
2.3	infPub	Contendrá la dirección del servicio web del órgano emisor al que se informará de la fecha de publicación de los anuncios y una dirección de correo electrónico. La forma de comunicar dicha información se tratará en documento aparte.		[1..1]	complexType
2.3.1	urlSW	Dirección del servicio web a la que se informará de la fecha de publicación de los anuncios.		[0..1]	anyUri
2.3.2	email	Dirección de correo electrónico a efectos de comunicar las incidencias que se generen en el proceso de la información.		[1..1]	string
2.4	anuncio	Este elemento puede repetirse ya que se admiten envíos con más de un anuncio. Cada elemento representará un anuncio distinto.		[1..*]	complexType
2.4.1	emisor	Organismo o unidad autor del anuncio. Contiene el árbol de la estructura del directorio DIR3 del organismo o unidad, incluyendo un elemento nodoEmisor para cada nivel. Nota: El organismo o unidad autor del anuncio no tiene que coincidir necesariamente con el remitente		[1..1]	complexType
2.4.1.1	nodoEmisor	Organismo o unidad autor del anuncio. Contiene dos atributos: idDir3: Código DIR3 del organismo. Tipo dato: string. nivel: Nivel dentro del árbol conforme a la estructura DIR3. Tipo dato: int. Por ejemplo, en el caso de la Agencia Estatal Boletín Oficial del Estado sería: <nodoEmisor nivel="1" idDir3="EA9999999">ADMINISTRACIÓN GENERAL DEL ESTADO</nodoEmisor> <nodoEmisor nivel="2" idDir3="E00004101">MINISTERIO DE LA PRESIDENCIA</nodoEmisor> <nodoEmisor nivel="3" idDir3="E00135501">SUBSECRETARIA DE LA PRESIDENCIA</nodoEmisor> <nodoEmisor nivel="4" idDir3="E04761001">AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO</nodoEmisor>		[1..*]	string
2.4.2	metadatos	Información que no se publicará pero indispensable para el tratamiento de los anuncios y la forma de publicarlos.		[1..1]	complexType
2.4.2.1	id	Identificador único del anuncio en los sistemas de información del órgano emisor. Aunque no es obligatorio, es indispensable para que se pueda informar al emisor de la fecha de publicación del anuncio. Es necesario si se ha incluido el elemento infPub/urlSW. Nota: Si no se ha proporcionado el dato y el elemento infPub/urlSW fue proporcionado se devolverá un aviso tras la recepción del XML pero no se detendrá la publicación. No será posible utilizar el servicio de Control de Publicación.		[0..1]	string
2.4.2.2	formPub	Forma de publicación. Es un dato obligatorio imprescindible para el tratamiento posterior y la forma de mostrar el anuncio. Puede tomar dos valores: E: Publicación en extracto (cuando el anuncio no contiene el contenido del acto administrativo a notificar, sino únicamente la identificación del interesado y del procedimiento) I: Publicación íntegra (cuando en el texto del anuncio se recoge completo el contenido del acto administrativo objeto de notificación)	[E],[I]	[1..1]	string
2.4.2.3	datosPersonales	Informa sobre si el anuncio contiene datos de carácter personal. Puede tomar los siguientes valores: N: No incluye ningún dato de carácter personal. S: Incluye datos de carácter personal.	[N],[S]	[1..1]	string
2.4.2.4	materias	Tipo de anuncio. Por ejemplo: "catastro", "impuestos", "tasas", "subvenciones" con el objetivo de facilitar la recuperación posterior en base de datos. Contendrá tantos elementos "materia" como sean precisos para facilitar la búsqueda del anuncio. Clasificación a determinar.		[0..1]	complexType

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
2.4.2.4.1	materia	Materia. Incluye el atributo idMat (tipo de datos string) con el identificador de la materia. Ejemplo: <materia idMat="12">tasas</materia> <materia idMat="23">catastro</materia>		[1..*]	string
2.4.2.5	lgt	El valor será "S" si el anuncio debe publicarse conforme a lo dispuesto en el artículo 112 de la Ley 58/2003 (Ley General Tributaria).	[S]	[0..1]	string
2.4.2.6	procedimiento	Identificación del procedimiento. Es un texto libre que permitirá construir de manera automatizada el título del anuncio y diferenciar entre los emitidos en igual fecha por el mismo emisor. Asimismo, una vez publicado el anuncio, facilitará la búsqueda por texto libre. Deberá incluir un atributo "plural" para indicar si debe emplearse el plural en la palabra procedimiento en el momento de generar el título del anuncio; para ello tomará el valor "S" para indicar el plural y "N" el singular. Se admitirá un máximo de 400 caracteres. No debe contener datos de carácter personal. Ejemplos (en primer lugar el bloque XML y a continuación el título del anuncio al que daría lugar): Ejemplo 1: <procedimiento plural="N">sancionador</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento sancionador Ejemplo 2: empleo del plural. En este ejemplo se incluye además un órgano que tramita el procedimiento. Este órgano debe ser un órgano distinto al emisor): <procedimiento plural="S"> tramitados por la Subdirección de.../departamento/Servicio de...</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimientos tramitados por la Subdirección de.../departamento/Servicio de... Ejemplo 3: <procedimiento plural="N"> nº de expediente xxx</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento nº de expediente xxx Ejemplo 4: <procedimiento plural="N"> de concesión de las subvenciones previstas en la Orden xxx, por la que se aprueban las correspondientes bases reguladoras</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento de concesión de las subvenciones previstas en la Orden xxx, por la que se aprueban las correspondientes bases reguladoras. Ejemplo 5: <procedimiento plural="N"> relativo a baja en el padrón municipal</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento relativo a baja en el padrón municipal Ejemplo 6 (correcciones de errores): <procedimiento plural="N"> relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores Ejemplo 7 (correcciones de errores): <procedimiento plural="N"> relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores del anuncio de notificación de 19 de julio</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores del anuncio de notificación de 19 de julio.		[0..1]	string
2.4.2.7	notificados	Aunque el elemento es opcional, deberá incluirse aquí la lista con los datos de los notificados si no es posible marcarlos en el elemento contenido/texto que se describe en el punto siguiente. Contendrá tantos elementos "notificado" como notificados haya.		[0..1]	complexType
2.4.2.7.1	notificado	Cada elemento notificado incluirá obligatoriamente el atributo id (tipo de dato string) que contendrá su identificación (normalmente el NIF) y el atributo tipId (tipo de dato string) para el tipo de identificador (NIF, NAF, CCC, EXP). Ejemplo: <notificado id="99999999R" tipId="NIF">Juan Español Español</notificado>		[1..*]	string
2.4.2.8	contenido	Contenido del anuncio.			complexType
2.4.2.8.1	texto	Texto del anuncio. Incluirá de forma obligatoria un atributo content-type (tipo de dato string) con el valor "application/xml" El nodo texto estará formado por dos tipos de nodos que pueden repetirse tantas veces como sea necesario: párrafos (p) y tablas (table). El anuncio debe contener al menos un elemento párrafo.		[1..1]	complexType
2.4.2.8.1.1	p	Párrafo de texto. Puede admitir un atributo class (tipo de dato string) para presentar la información. Este atributo puede tomar los siguientes valores: parrafo: Párrafo por defecto. titulo: Párrafo centrado con un tipo de letra mayor que el del párrafo por defecto. pieFirma: El elemento no tendrá contenido alguno. Representa la posición donde se incorporá el texto del elemento pieFirma. De no incluirse, el pie de firma irá al final del texto. page-break: El elemento no tendrá contenido alguno. Fuerza un salto de página a partir de este elemento. Si no se indica el atributo, se le aplicará el atributo del párrafo por defecto. Ejemplos: Este es un párrafo normal Este es otro párrafo normal ANEXO		[1..*]	string
2.4.2.8.1.1.1	span	Dentro de un párrafo se podrán incluir elementos span con el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC, EXP o un nombre, para marcar un contenido a indexar si este no se ha incluido en el apartado metadatos/notificados. Por ejemplo: Se notifica a Juan Español Español con NIF 99999999R lo siguiente....			string
2.4.2.8.1.2	table	Tabla con información		[0..*]	complexType
2.4.2.8.1.2.1	caption	Título de la tabla		[0..1]	string
2.4.2.8.1.2.2	colgroup	Contiene información de las columnas de la tabla. Debe contener tantos elementos col como columnas tenga la tabla.		[0..1]	complexType

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
2.4.2.8.1.2.2.1	col	En él podrá especificarse si el contenido de la columna deberá ser indexado e incorporado al buscador añadiéndole el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC o un nombre. Ejemplo: <colgroup> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col /> <col /> <col /> </colgroup> En este ejemplo las columnas 1 y 3 de la tabla incluyen un NIF y las 2 y 4 un NOMBRE que deben incorporarse al buscador. Las columnas 5, 6 y 7 no se incorporarán al buscador.		[1..*]	complexType
2.4.2.8.1.2.3	thead	Cabecera de la tabla.		[0..1]	complexType
2.4.2.8.1.2.3.1	tr	Fila de la cabecera		[1..*]	complexType
2.4.2.8.1.2.3.1.1	th	Celda de la cabecera. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.8.1.2.4	tbody	Cuerpo de la tabla.		[1..1]	complexType
2.4.2.8.1.2.4.1	tr	Fila de la tabla		[1..*]	complexType
2.4.2.8.1.2.4.1.1	td	Celda de la tabla. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.8.1.2.5	tfoot	Pie de la tabla. Normalmente no se usará.		[0..1]	complexType
2.4.2.8.1.2.5.1	tr	Fila del pie		[1..*]	complexType
2.4.2.8.1.2.5.1.1	th	Celda del pie. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.8.2	pieFirma	Pie de firma del anuncio Ejemplo 1: <pieFirma> <lugar>Madrid</lugar> <fecha>2014-08-19</fecha> <firmante>El Jefe de Servicio de Pruebas, Juan Español Español </firmante> </pieFirma> Ejemplo 2: <pieFirma> <lugar>Madrid</lugar> <fecha>2014-08-19</fecha> <firmante>El Subdirector General del Servicio de Pruebas, P.D. (Orden PRE/127/2013, de 3 de mayo), el Jefe del Servicio de Pruebas, Juan Español Español</firmante> </pieFirma>		[1..1]	complexType
2.4.2.8.2.1	lugar	Población en que tiene lugar la firma		[1..1]	string
2.4.2.8.2.2	fecha	Fecha de la firma en formato ISO 8601:2004 (aaaa-mm-dd).		[1..1]	string
2.4.2.8.2.3	firmante	Cargo y nombre y dos apellidos del firmante. En los casos de actuación administrativa automatizada puede consistir únicamente en la identificación del organismo o unidad firmante. En casos de alteración de la competencia deberán incluirse las referencias correspondientes. Este elemento debe estar informado.		[1..1]	string
2.4.2.9	contenidoCoof	Contenido del anuncio en lengua cooficial.		[0..1]	complexType
2.4.2.9.1	texto	Texto del anuncio. Incluirá de forma obligatoria un atributo content-type (tipo de dato string) con el valor "application/xml" El nodo texto estará formado por dos tipos de nodos que pueden repetirse tantas veces como sea necesario: párrafos (p) y tablas (table). El anuncio debe contener al menos un elemento párrafo. Si el texto cooficial lleva firma, debe ser incluido dentro de este elemento.		[1..1]	complexType
2.4.2.9.1.1	p	Párrafo de texto. Puede admitir un atributo class (tipo de dato string) para presentar la información. Este atributo puede tomar los siguientes valores: parrafo: Párrafo por defecto. titulo: Párrafo centrado con un tipo de letra mayor que el del párrafo por defecto. page-break: El elemento no tendrá contenido alguno. Fuerza un salto de página a partir de este elemento. Si no se indica el atributo, se le aplicará el atributo del párrafo por defecto. Ejemplos: Este es un párrafo normal Este es otro párrafo normal ANEXO		[1..*]	string
2.4.2.9.1.1.1	span	Dentro de un párrafo se podrán incluir elementos span con el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC, EXP o un nombre, para marcar un contenido a indexar si este no se ha incluido en el apartado metadatos/notificados. Por ejemplo: Se notifica a Juan Español Español con NIF 99999999R lo siguiente....			string
2.4.2.9.1.2	table	Tabla con información		[0..*]	complexType
2.4.2.9.1.2.1	caption	Título de la tabla		[0..1]	string
2.4.2.9.1.2.2	colgroup	Contiene información de las columnas de la tabla. Debe contener tantos elementos col como columnas tenga la tabla.		[0..1]	complexType

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
2.4.2.9.1.2.2.1	col	En él podrá especificarse si el contenido de la columna deberá ser indexado e incorporado al buscador añadiéndole el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC o un nombre. Ejemplo: <colgroup> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col /> <col /> <col /> </colgroup> En este ejemplo las columnas 1 y 3 de la tabla incluyen un NIF y las 2 y 4 un NOMBRE que deben incorporarse al buscador. Las columnas 5, 6 y 7 no se incorporarán al buscador.		[1..*]	complexType
2.4.2.9.1.2.3	thead	Cabecera de la tabla.		[0..1]	complexType
2.4.2.9.1.2.3.1	tr	Fila de la cabecera		[1..*]	complexType
2.4.2.9.1.2.3.1.1	th	Celda de la cabecera. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.9.1.2.4	tbody	Cuerpo de la tabla.		[1..1]	complexType
2.4.2.9.1.2.4.1	tr	Fila de la tabla		[1..*]	complexType
2.4.2.9.1.2.4.1.1	td	Celda de la tabla. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.9.1.2.5	tfoot	Pie de la tabla. Normalmente no se usará.		[0..1]	complexType
2.4.2.9.1.2.5.1	tr	Fila del pie		[1..*]	complexType
2.4.2.9.1.2.5.1.1	th	Celda del pie. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string"

ANEXO II

Formato XML para el envío de los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único

El contenido del envío se realizará en formato XML con la información estructurada de la siguiente forma:

```
<envio>
    <version>
    <remitente>
    <fechaPub>?
    <controlPub>
        <url>
        <email>
    </controlPub>
    <edictos>
        <edicto>+
            <emisor>
            <metadatos>?
                <id>?
                <sede>?
            </metadatos>
            <organo>
                <identificacion>
                <direccion>
                <localidad>
                <cp>
                <provincia>
                <telefono>?
                <email>?
            </organo>
            <contenido>+
                <procedimiento>
                    <tipo>
                    <numero>
                    <nig>
                </procedimiento>
                <resolucion>+
                    <tipo>
                    <fecha>
                    <objeto>+
                        <tipo>
                        <plazo>?<p></plazo>
                    </objeto>
```

```
                    </resolucion>
                    <destinatarios>?
                        <determinados>
                            <nombre>
                        </determinados>
                        <indeterminados>
                            <p>+
                        </indeterminados>
                    </destinatarios>
                    <observaciones>?
                        <p>+
                    </observaciones>
                </contenido>
                <firma>
                    <lugar>
                    <fecha>
                    <cargo>
                    <firmante>
                </firma>
            </edicto>
        </edictos>
    </envio>
```

+ significa una o más ocurrencias.
? significa cero o una ocurrencia.
* significa cero o más ocurrencias.

A continuación se describen de forma pormenorizada cada uno de los elementos.

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
	envio	Nodo raíz del envío.		[1..1]	
1	version	Código que indica la versión utilizada. Existirá compatibilidad de versiones.	[1.0.0]	[1..1]	string
2	remitente	Código del órgano judicial remitente del edicto, que puede ser el mismo que el emisor o el de un servicio común que actúe como remitente de edictos emitidos por otros órganos judiciales.		[1..1]	string
3	fechaPub	Fecha de publicación solicitada en formato ISO 8601:2004 (aaaa-mm-dd).		[0..1]	string
4	controlPub	Información de control de publicación o devolución.		[1..1]	complexType
4.1	url	Dirección del servicio web a la que se informará de la fecha de publicación de los edictos o de su devolución.		[0..1]	anyUri
4.2	email	Dirección de correo electrónico a la que se informará la fecha de publicación de los edictos o de su devolución.		[1..1]	string
5	edictos	Lista de edictos que componen el envío.		[1..1]	complexType
5.1	edicto	Información relativa a un edicto.		[1..*]	complexType
5.1.1	emisor	Código del órgano judicial que emite el edicto *Nota: El emisor y el remitente será el mismo órgano judicial, salvo en el caso de los servicios comunes que actúen como remitentes de edictos emitidos por otros órganos judiciales.*		[1..1]	string
5.1.2	metadatos	Información que facilita la identificación de los edictos en los sistemas de información y su localización en la sede electrónica correspondiente.		[0..1]	complexType
5.1.2.1	id	Identificador único del edicto en los sistemas de información del órgano emisor o remitente. Este campo es opcional, aunque se recomienda que esté informado porque permite identificar posibles envíos de edictos duplicados.		[0..1]	string
5.1.2.2	sede	URL de la sede electrónica donde se encuentra disponible el edicto.		[0..1]	anyUri
5.1.3	organo	Datos del órgano emisor.		[1..1]	complexType
5.1.3.1	identificacion	Descripción textual (nombre) del órgano judicial.		[1..1]	string
5.1.3.2	direccion	Domicilio del órgano judicial.		[1..1]	string
5.1.3.3	localidad	Localidad del órgano judicial.		[1..1]	string
5.1.3.4	provincia	Código de provincia del órgano judicial. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.3.5	telefono	Teléfono del órgano judicial.		[0..1]	string
5.1.3.6	email	Dirección de correo electrónico del órgano judicial.		[0..*]	string
5.1.4	contenido	Contenido del edicto. Incluye el atributo idioma con el identificador del idioma en el que está escrito el edicto. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE. Pueden incluirse dos elementos de este tipo si el edicto se publica en lengua cooficial, además del castellano. En ese caso, ambos elementos tendrán los mismos valores, salvo para los campos «plazo» y «observaciones», que deberán ser redactados en la lengua correspondiente.		[1..2]	complexType
5.1.4.1	procedimiento	Datos del procedimiento.		[1..1]	complexType
5.1.4.1.1	tipo	Código del tipo de procedimiento. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.4.1.2	numero	Número de procedimiento, compuesto por el año (expresado con 4 dígitos) y el número secuencial dentro del año.		[1..1]	string
5.1.4.1.3	nig	Número de identificación general.		[0..1]	string
5.1.4.2	resolucion	Datos de la resolución.		[1..*]	complexType
5.1.4.2.1	tipo	Código del tipo de resolución. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.4.2.2	fecha	Fecha de la resolución en formato ISO 8601:2004 (aaaa-mm-dd).		[1..1]	string
5.1.4.2.3	objeto	Objeto del edicto.		[1..*]	complexType
5.1.4.2.3.1	tipo	Tipo de objeto, cuya tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.4.2.3.2	plazo	Indicaciones relativas al plazo para atender el tipo de objeto.		[0..1]	string
5.1.4.2.3.2.1	p	Párrafo de texto en el que se incluye las indicaciones relativas al plazo.		[1..1]	string
5.1.4.3	destinatarios	Identificación de los destinatarios del edicto. Si existe este elemento, tiene que incluir o bien el elemento «determinados» o bien el elemento «indeterminados».		[0..*]	complexType

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
5.1.4.3.1	determinados	Identificación de los destinatarios determinados del edicto, si existen.		[1..1]	complexType
5.1.4.3.1.1	nombre	Nombre del destinatario. Incluye tres atributos para determinar la identificación: 1. tipoId: Tipo de identificador del destinatario, cuya tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE 2. id: Número de identificador 3. truncado: Permite que el órgano judicial indique si el número de identificador debe publicarse de forma íntegra o parcial.		[1..*]	string
5.1.4.3.2	indeterminados	Descripción de los destinatarios indeterminados del edicto.		[1..1]	complexType
5.1.4.3.2.1	p	Párrafo de texto con la descripción de los destinatarios indeterminados.		[1..*]	string
5.1.4.4	observaciones	Observaciones del emisor.		[0..1]	complexType
5.1.4.4.1	p	Párrafo de texto para que el órgano judicial incorpore la información complementaria que debe aparecer en el edicto.		[1..*]	string
5.1.5	firma	Pie de firma del anuncio.		[1..1]	complexType
5.1.5.1	lugar	Población en que tiene lugar la firma.		[1..1]	string
5.1.5.2	fecha	Fecha de la firma en formato ISO 8601:2004 (aaaa-mm-dd).		[1..1]	string
5.1.5.3	cargo	Código del cargo del firmante. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.5.4	firmante	Nombre y dos apellidos del firmante.		[1..1]	string

§ 33

Ley de 18 de junio de 1870 estableciendo reglas para el ejercicio de la gracia de indulto

Ministerio de Gracia y Justicia
«Gaceta de Madrid» núm. 175, de 24 de junio de 1870
Última modificación: 31 de marzo de 2015
Referencia: BOE-A-1870-4759

CAPÍTULO I

De los que pueden ser indultados

Artículo 1.

Los reos de toda clase de delitos podrán ser indultados, con arreglo a las disposiciones de esta Ley, de toda o parte de la pena en que por aquéllos hubiesen incurrido.

Artículo 2.

Se exceptúan de lo establecido en el artículo anterior:

1.º Los procesados criminalmente que no hubieren sido aún condenados por sentencia firme.

2.º Los que no estuvieren a disposición del Tribunal sentenciador para el cumplimiento de la condena.

3.º Los reincidentes en el mismo o en otro cualquiera delito por el cual hubiesen sido condenados por sentencia firme. Se exceptúa, sin embargo, el caso en que, a juicio del Tribunal sentenciador hubiera razones suficientes de justicia, equidad o conveniencia pública para otorgarle la gracia.

Artículo 3.

Lo dispuesto en el artículo anterior no será aplicable a los penados por delitos comprendidos en el capítulo I, secciones primera y segunda del capítulo II, y en los capítulos III, IV y V, todos del título II del libro II del Código Penal.

CAPÍTULO II

De las clases y efectos del indulto

Artículo 4.

El indulto podrá ser total o parcial.

Será indulto total la remisión de todas las penas a que hubiese sido condenado y que todavía no hubiese cumplido el delincuente.

Será indulto parcial la remisión de alguna o algunas de las penas impuestas, o de parte de todas en que hubiese incurrido y no hubiese cumplido todavía el delincuente.

Se reputará también indulto parcial la conmutación de la pena o penas impuestas al delincuente en otras menos graves.

Artículo 5.

Será nula y no producirá efecto ni deberá ejecutarse por el Tribunal a quien corresponda la concesión del indulto en que no se hiciese mención expresa a lo menos de la pena principal sobre que recaiga la gracia.

Artículo 6.

El indulto de la pena principal llevará consigo el de las accesorias que con ella se hubiesen impuesto al penado, a excepción de las de inhabilitación para cargos públicos y derechos políticos y sujeción a la vigilancia de la Autoridad, las cuales no se tendrán por comprendidas si de ellas no se hubiese hecho mención especial en la concesión.

Tampoco se comprenderá nunca en ésta la indemnización civil.

Artículo 7.

Podrá concederse indulto de las penas accesorias, con exclusión de las principales y viceversa, a no ser de aquellas que sean inseparables por su naturaleza y efectos.

Artículo 8.

El indulto de pena pecuniaria eximirá al indultado del pago de la cantidad que aún no hubiese satisfecho, pero no comprenderá la devolución de la ya pagada, a no ser que así se determine expresamente.

Artículo 9.

El indulto no se extenderá a las costas procesales.

Artículo 10.

Si el penado hubiere fallecido al tiempo o después de existir causas bastantes para la concesión de su indulto, podrá relevarse a sus herederos de la pena accesoria de multa, con arreglo a lo dispuesto en los artículos 8.º y 9.º

Artículo 11.

El indulto total se otorgará a los penados tan sólo en el caso de existir a su favor razones de justicia, equidad o utilidad pública, a juicio del Tribunal sentenciador.

Artículo 12.

En los demás casos se concederá tan sólo el parcial, y con preferencia la conmutación de la pena impuesta en otra menos grave dentro de la misma escala gradual.

Sin embargo, de lo dispuesto en el párrafo anterior, podrá también conmutarse la pena en otra de distinta escala cuando haya méritos suficientes para ello, a juicio del Tribunal sentenciador o del Consejo de Estado, y el penado además se conformare con la conmutación.

Artículo 13.

Conmutada la pena principal, se entenderán también conmutadas las accesorias por las que correspondan, según las prescripciones del Código, a la que hubiere de sufrir el indultado.

Se exceptúa, sin embargo, el caso en que se hubiese dispuesto otra cosa en la concesión de la gracia.

Artículo 14.

La conmutación de la pena quedará sin efecto desde el día en que el indultado deje de cumplir, por cualquiera causa dependiente de su voluntad, la pena a que por la conmutación hubiere quedado sometido.

Artículo 15.

Serán condiciones tácitas de todo indulto:

1.ª Que no cause perjuicio a tercera persona, o no lastime sus derechos.

2.ª Que haya sido oída la parte ofendida, cuando el delito por que hubiese sido condenado el reo fuere de los que solamente se persiguen a instancia de parte.

Artículo 16.

Podrán, además, imponerse al penado en la concesión de la gracia las demás condiciones que la justicia, la equidad o la utilidad pública aconsejen.

Artículo 17.

El Tribunal sentenciador no dará cumplimiento a ninguna concesión de indulto cuyas condiciones no hayan sido previamente cumplidas por el penado; salvo las que por su naturaleza no lo permitan.

Artículo 18.

La concesión del indulto es por su naturaleza irrevocable con arreglo a las cláusulas con que hubiere sido otorgado.

CAPÍTULO III

Del procedimiento para solicitar y conceder la gracia del indulto

Artículo 19.

Pueden solicitar el indulto los penados, sus parientes o cualquiera otra persona en su nombre, sin necesidad de poder escrito que acredite su representación.

Artículo 20.

Puede también proponer el indulto el Tribunal sentenciador, o el Tribunal Supremo, o el Fiscal de cualquiera de ellos, con arreglo a lo que se dispone en el párrafo tercero, art. 2.º del Código Penal, y se disponga además en las Leyes de procedimientos y casación criminal.

La propuesta será reservada hasta que el Ministro de Justicia en su vista, decrete la formación del oportuno expediente.

Artículo 21.

Podrá también el Gobierno mandar formar el oportuno expediente, con arreglo a las disposiciones de esta Ley, para la concesión de indultos que no hubiesen sido solicitados por los particulares ni propuestos por los Tribunales de Justicia.

Artículo 22.

Las solicitudes de indultos se dirigirán al Ministro de Justicia por conducto del Tribunal sentenciador, del Jefe del Establecimiento o del Gobernador de la provincia en que el penado se halle cumpliendo la condena, según los respectivos casos.

Artículo 23.

Las solicitudes de indulto, inclusas las que directamente se presentaren al Ministro de Justicia, se remitirán a informe del Tribunal sentenciador.

Artículo 24.

Este pedirá, a su vez, informe sobre la conducta del penado al Jefe del establecimiento en que aquél se halle cumpliendo la condena, o al Gobernador de la provincia de su residencia, si la pena no consistiese en la privación de libertad, y oirá después al Fiscal y a la parte ofendida si la hubiere.

Artículo 25.

El Tribunal sentenciador hará constar en su informe, siendo posible, la edad, estado y profesión del penado, su fortuna si fuere conocida, sus méritos y antecedentes, si el penado fue con anterioridad procesado y condenado por otro delito, y si cumplió la pena impuesta o fue de ella indultado, por qué causa y en qué forma, las circunstancias agravantes o atenuantes que hubiesen concurrido en la ejecución del delito, el tiempo de prisión preventiva que hubiese sufrido durante la causa, la parte de la condena que hubiere cumplido, su conducta posterior a la ejecutoria, y especialmente las pruebas o indicios de su arrepentimiento que se hubiesen observado, si hay o no parte ofendida, y si el indulto perjudica el derecho de tercero, y cualesquiera otros datos que puedan servir para el mejor esclarecimiento de los hechos, concluyendo por consignar su dictamen sobre la justicia o conveniencia y forma de la concesión de la gracia.

Artículo 26.

El Tribunal sentenciador remitirá con su informe al Ministro de Justicia la hoja histórico-penal y el testimonio de la sentencia ejecutoria del penado, con los demás documentos que considere necesarios para la justificación de los hechos.

Artículo 27.

Los Tribunales Supremo o sentenciador que de oficio propongan al Gobierno el indulto de un penado, acompañarán desde luego con la propuesta el informe y documentos a que se refieren los artículos anteriores.

Artículo 28.

Los expedientes que se formen al amparo del párrafo segundo del artículo 2.º del Código Penal se tramitarán en turno preferente cuando los informes del Ministerio Fiscal y del Establecimiento Penitenciario y del ofendido, en su caso, no se opusieran a la propuesta del Tribunal.

También se tramitarán en turno preferente los expedientes calificados de especial urgencia o importancia.

Artículo 29.

Sin embargo de lo dispuesto en los artículos anteriores, podrá concederse la conmutación de la pena de muerte y las impuestas por los delitos comprendidos en los capítulos 1.° y 2.°, tít. 2.°, libro 2.°, y capítulos 1.°, 2.° y 3.°, tít. 3.° del mismo, libro del Código penal últimamente reformado, sin oir previamente al Tribunal sentenciador.

Artículo 30.

La concesión de los indultos, cualquiera que sea su clase, se hará en Real Decreto, que se insertará en el «Boletín Oficial del Estado».

Artículo 31.

La aplicación de la gracia habrá de encomendarse indispensablemente al Tribunal sentenciador.

Artículo 32.

La solicitud o propuesta de indulto no suspenderá el cumplimiento de la sentencia ejecutoria, salvo el caso en que la pena impuesta fuese la de muerte, la cual no se ejecutará

hasta que el Gobierno haya acusado el recibo de la solicitud o propuesta al Tribunal sentenciador.

Disposición adicional.

El Gobierno remitirá semestralmente al Congreso de los Diputados un informe sobre la concesión y denegación de indultos. Para la presentación de los datos contenidos en el citado informe, y previa revisión del mismo, un alto cargo del Ministerio de Justicia solicitará su comparecencia ante la Comisión de Justicia del Congreso de los Diputados.

§ 34

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 63, de 14 de marzo de 1986
Última modificación: 29 de julio de 2015
Referencia: BOE-A-1986-6859

TÍTULO I

De los Cuerpos y Fuerzas de Seguridad

[. . .]

CAPÍTULO II

Principios básicos de actuación

Artículo quinto.

Son principios básicos de actuación de los miembros de las Fuerzas y Cuerpos de Seguridad los siguientes:

1. Adecuación al ordenamiento jurídico, especialmente:

a) Ejercer su función con absoluto respeto a la Constitución y al resto del ordenamiento jurídico.

b) Actuar, en el cumplimiento de sus funciones, con absoluta neutralidad política e imparcialidad y, en consecuencia, sin discriminación alguna por razón de raza, religión u opinión.

c) Actuar con integridad y dignidad. En particular, deberán abstenerse de todo acto de corrupción y oponerse a él resueltamente.

d) Sujetarse en su actuación profesional, a los principios de jerarquía y subordinación. En ningún caso, la obediencia debida podrá amparar órdenes que entrañen la ejecución de actos que manifiestamente constituyan delito o sean contrarios a la Constitución o a las Leyes.

e) Colaborar con la Administración de Justicia y auxiliarla en los términos establecidos en la Ley.

2. Relaciones con la comunidad. Singularmente:

a) Impedir, en el ejercicio de su actuación profesional, cualquier práctica abusiva, arbitraria o discriminatoria que entrañe violencia física o moral.

b) Observar en todo momento un trato correcto y esmerado en sus relaciones con los ciudadanos, a quienes procurarán auxiliar y proteger, siempre que las circunstancias lo

aconsejen o fueren requeridos para ello. En todas sus intervenciones, proporcionarán información cumplida, y tan amplia como sea posible, sobre las causas y finalidad de las mismas.

c) En el ejercicio de sus funciones deberán actuar con la decisión necesaria, y sin demora cuando de ello dependa evitar un daño grave, inmediato e irreparable; rigiéndose al hacerlo por los principios de congruencia, oportunidad y proporcionalidad en la utilización de los medios a su alcance.

d) Solamente deberán utilizar las armas en las situaciones en que exista un riesgo racionalmente grave para su vida, su integridad física o las de terceras personas, o en aquellas circunstancias que puedan suponer un grave riesgo para la seguridad ciudadana y de conformidad con los principios a que se refiere el apartado anterior.

3. Tratamiento de detenidos, especialmente:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad deberán identificarse debidamente como tales en el momento de efectuar una detención.

b) Velarán por la vida e integridad física de las personas a quienes detuvieren o que se encuentren bajo su custodia y respetarán el honor y la dignidad de las personas.

c) Darán cumplimiento y observarán con la debida diligencia los trámites, plazos y requisitos exigidos por el ordenamiento jurídico, cuando se proceda a la detención de una persona.

4. Dedicación profesional.

Deberán llevar a cabo sus funciones con total dedicación, debiendo intervenir siempre, en cualquier tiempo y lugar, se hallaren o no de servicio, en defensa de la Ley y de la seguridad ciudadana.

5. Secreto profesional.

Deberán guardar riguroso secreto respecto a todas las informaciones que conozcan por razón o con ocasión del desempeño de sus funciones. No estarán obligados a revelar las fuentes de información salvo que el ejercicio de sus funciones o las disposiciones de la Ley les impongan actuar de otra manera.

6. Responsabilidad.

Son responsables personal y directamente por los actos que en su actuación profesional llevaren a cabo, infringiendo o vulnerando las normas legales, así como las reglamentarias que rijan su profesión y los principios enunciados anteriormente, sin perjuicio de la responsabilidad patrimonial que pueda corresponder a las Administraciones Públicas por las mismas.

[. . .]

Artículos dieciséis a veintiocho.

(Derogados)

[. . .]

Sexta. *Carácter de ley orgánica.*

Tienen el carácter de ley orgánica los preceptos que se contienen en los títulos I, III, IV y V y en el título II, salvo los artículos 10, 11.2 a 6 y 12.1, la disposición adicional tercera y las disposiciones finales, excepto la disposición final quinta.

[. . .]

§ 35

Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN

Jefatura del Estado
«BOE» núm. 242, de 9 de octubre de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-17634

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

El ácido desoxirribonucleico (ADN), componente químico del núcleo celular, se ha convertido en un instrumento esencial de las técnicas que la moderna medicina forense utiliza para la investigación de delitos por parte de las autoridades judiciales y policiales.

Desde que en 1988, en el Reino Unido y por primera vez, la información obtenida del ADN fuese utilizada para identificar y condenar al culpable de un delito, tanto en España como en el resto de los países de nuestro entorno se ha tomado conciencia de la trascendencia de los marcadores genéticos en las investigaciones criminales, algo que venía siendo más frecuente en otros ámbitos, como la identificación de cadáveres o la determinación de relaciones de parentesco.

Sin embargo, y a pesar de esa importancia, el uso de los datos relacionados con el ADN, en el ámbito de la persecución de delitos, cuenta hoy con numerosas dificultades, especialmente en lo relativo a su obtención y registro de cara a su empleo en el curso de ulteriores investigaciones. Ello viene dado tanto por el carácter sensible que dichos datos tienen y el importante grado de protección con que, naturalmente, deben contar, como por la inexistencia de un marco jurídico que regule adecuadamente su empleo.

En el año 2003, y mediante lo dispuesto en la Disposición Final Primera de la Ley Orgánica 15/2003, de 25 de noviembre, de modificación del Código Penal, se reformó la Ley de Enjuiciamiento Criminal a fin de proporcionar cobertura jurídica, de la que carecían hasta entonces, a determinadas prácticas de investigación.

La nueva redacción dada a los artículos 326 y 363 de la Ley de Enjuiciamiento Criminal consistió, esencialmente, en regular la posibilidad de obtener el ADN a partir de muestras biológicas provenientes de pruebas halladas en el lugar del delito o extraídas de

sospechosos, de manera que dichos perfiles de ADN puedan ser incorporados a una base de datos para su empleo en esa concreta investigación.

Sin embargo, la reforma no contempló otros aspectos importantes, como la posibilidad de crear una base de datos en la que, de manera centralizada e integral, se almacenase el conjunto de los perfiles de ADN obtenidos, a fin de que pudiesen ser utilizados, posteriormente, en investigaciones distintas o futuras, incluso sin el consentimiento expreso del titular de los datos.

Estas carencias, unidas a otros factores de naturaleza diversa, ponen de manifiesto la insuficiencia de la regulación vigente para satisfacer tanto las posibilidades técnicas y las demandas ciudadanas, como los compromisos internacionales progresivamente adquiridos por nuestro país en materia de intercambio de perfiles de ADN para las investigaciones de determinados delitos.

Por un lado, resulta indudable que los avances técnicos permiten hoy que la obtención de datos exclusivamente identificativos a partir de una muestra de ADN se pueda realizar de manera rápida, económica y escasamente limitadora de los derechos ciudadanos. Por otro, la sociedad viene exigiendo que las autoridades, judiciales y policiales, encargadas de la persecución de los delitos, cuenten con los instrumentos de investigación más eficientes posibles, especialmente en la lucha contra aquellos crímenes que generan mayor alarma social. Finalmente, no puede olvidarse que la creciente globalización de los delitos y la paralela asunción por parte de España de una serie de obligaciones recíprocas con otros países para compartir la información disponible en los respectivos ficheros y bases de datos exigen la adopción de las medidas materiales y jurídicas adecuadas.

Respecto de este último aspecto, cabe señalar que la adopción de esas medidas jurídicas, así como la creación de bases de datos que permitan intercambiar la información entre los Estados miembros, ha sido reiteradamente expuesta desde las Instituciones comunitarias a través de sendas Resoluciones del Consejo relativas al intercambio de resultados de análisis de ADN, de 9 de junio de 1997 y de 25 de julio de 2001, respectivamente. En el mismo sentido se ha venido pronunciando el Consejo de Europa a partir de la Recomendación (92) 1, de 10 de febrero de 1992, de su Comité de Ministros, sobre la utilización de los resultados de análisis de ADN en el marco del sistema de justicia penal.

Finalmente, debe recalcarse que en la redacción de la presente Ley, como no podría ser de otra manera, se han tenido en cuenta los criterios que, sobre la protección de los derechos fundamentales en la obtención de pruebas a partir de los perfiles de ADN, ha venido conformando el Tribunal Constitucional en diversas Sentencias como la 207/1996, de 16 de diciembre.

II

El articulado de la presente Ley comienza determinando lo que constituye su objetivo fundamental, que no es otro que la creación de una base de datos en la que, de manera única, se integren los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado en los que se almacenan los datos identificativos obtenidos a partir de los análisis de ADN que se hayan realizado en el marco de una investigación criminal, o en los procedimientos de identificación de cadáveres o de averiguación de personas desaparecidas.

En relación con su integración orgánica, la base de datos policiales sobre identificadores obtenidos a partir del ADN dependerá del Ministerio del Interior a través de la Secretaría de Estado de Seguridad.

A continuación, la Ley incorpora una importante novedad, ya que posibilita que para determinados delitos de especial gravedad y repercusión social -así como en el caso de los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de personas desaparecidas, o cuando el titular de los datos haya prestado su consentimiento para la inscripción-, los resultados obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, sean inscritos y conservados en la base de datos policial, a fin de que puedan ser utilizados en esa concreta investigación, o en otras que se sigan por la comisión de alguno de los delitos para los que la propia Ley habilita la inscripción de los perfiles de ADN en la base de datos.

Esta regulación contiene una salvaguarda muy especial, que resulta fundamental para eliminar toda vulneración del derecho a la intimidad, puesto que sólo podrán ser inscritos aquellos perfiles de ADN que sean reveladores, exclusivamente, de la identidad del sujeto -la misma que ofrece una huella dactilar- y del sexo, pero, en ningún caso, los de naturaleza codificante que permitan revelar cualquier otro dato o característica genética.

Otra importante garantía técnica se deriva de la exigencia que la Ley establece en relación con la obligatoria acreditación con que deberán contar los laboratorios que vayan a realizar los correspondientes análisis biológicos, siendo competente para conceder dicha acreditación, de acuerdo con la Disposición Adicional Tercera de la Ley de Enjuiciamiento Criminal, la Comisión Nacional para el uso forense del ADN.

En relación con el período de la conservación de los perfiles identificativos en la base de datos, la Ley fija unos períodos de cancelación cuya duración dependerá del tipo del delito y de la resolución judicial con que finalice el procedimiento penal.

A fin de alcanzar el objetivo de que la base de datos creada sea lo más completa y eficaz posible, se dispone no sólo que el Ministerio del Interior adopte las medidas oportunas para que los diferentes ficheros y bases de datos de ADN que, en el ámbito de las Fuerzas y Cuerpos de Seguridad del Estado existieran en el momento de su entrada en vigor, pasen a integrarse en la base de datos que la presente Ley crea, sino que también que puedan, eventualmente, integrarse en un futuro, y mediante la suscripción del correspondiente Convenio, otros ficheros, registros o bases de datos identificativos obtenidos a partir del ADN, que no dependan de las Fuerzas y Cuerpos de Seguridad del Estado.

Por último, el texto se inscribe en el marco de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, por su propia naturaleza de regulación general en la materia, resulta de aplicación directa, siendo los preceptos de esta Ley especialidades permitidas por la citada Ley Orgánica, que encontrarían su justificación en las peculiaridades de la base de datos que regula.

Artículo 1. *Creación.*

Se crea la base de datos policial de identificadores obtenidos a partir del ADN, que integrará los ficheros de esta naturaleza de titularidad de las Fuerzas y Cuerpos de Seguridad del Estado tanto para la investigación y averiguación de delitos, como para los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas.

Artículo 2. *Dependencia orgánica.*

La base de datos policial de identificadores obtenidos a partir del ADN dependerá del Ministerio del Interior, a través de la Secretaría de Estado de Seguridad.

Artículo 3. *Tipos de identificadores obtenidos a partir del ADN incluidos en la base de datos policial.*

1. Se inscribirán en la base de datos policial de identificadores obtenidos a partir del ADN los siguientes datos:

a) Los datos identificativos extraídos a partir del ADN de muestras o fluidos que, en el marco de una investigación criminal, hubieran sido hallados u obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados.

b) los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas.

La inscripción en la base de datos policial de los identificadores obtenidos a partir del ADN a que se refiere este apartado, no precisará el consentimiento del afectado, el cual será

informado por escrito de todos los derechos que le asisten respecto a la inclusión en dicha base, quedando constancia de ello en el procedimiento.

2. Igualmente, podrán inscribirse los datos identificativos obtenidos a partir del ADN cuando el afectado hubiera prestado expresamente su consentimiento.

Artículo 4. *Tipos de datos.*

Sólo podrán inscribirse en la base de datos policial regulada en esta Ley los identificadores obtenidos a partir del ADN, en el marco de una investigación criminal, que proporcionen, exclusivamente, información genética reveladora de la identidad de la persona y de su sexo.

Artículo 5. *Laboratorios acreditados.*

1. Las muestras o vestigios tomados respecto de los que deban realizarse análisis biológicos, se remitirán a los laboratorios debidamente acreditados. Corresponderá a la autoridad judicial pronunciarse sobre la ulterior conservación de dichas muestras o vestigios.

2. Sólo podrán realizar análisis del ADN para identificación genética en los casos contemplados en esta Ley los laboratorios acreditados a tal fin por la Comisión Nacional para el uso forense del ADN que superen los controles periódicos de calidad a que deban someterse.

Artículo 6. *Remisión de los datos.*

La remisión de los datos identificativos obtenidos a partir del ADN, para su inscripción en la base de datos policial en los supuestos establecidos en el artículo 3 de esta Ley, se efectuará por la Policía Judicial, adoptándose para ello todas las garantías legales que aseguren su traslado, conservación y custodia.

Artículo 7. *Uso y cesión de los datos contenidos en la base de datos.*

1. Los datos contenidos en la base de datos objeto de esta Ley sólo podrán utilizarse por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas de la Policía y de la Guardia Civil en el ejercicio de las funciones previstas en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, así como por las Autoridades Judiciales y Fiscales, en la investigación de los delitos enumerados en la letra a) del apartado primero del artículo 3 de esta Ley.

2. No obstante lo dispuesto en el apartado anterior, cuando el tratamiento se realizase para la identificación de cadáveres o la averiguación de personas desaparecidas, los datos incluidos en la base de datos objeto de esta Ley sólo podrán ser utilizados en la investigación para la que fueron obtenidos.

3. Podrán cederse los datos contenidos en la base de datos:

a) A las Autoridades Judiciales, Fiscales o Policiales de terceros países de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes.

b) A las Policías Autonómicas con competencia estatutaria para la protección de personas y bienes y para el mantenimiento de la seguridad pública, que únicamente podrán utilizar los datos para la investigación de los delitos enumerados en la letra a) del apartado 1 del artículo 3 de esta Ley o, en su caso, para la identificación de cadáveres o averiguación de personas desaparecidas.

c) Al Centro Nacional de Inteligencia, que podrá utilizar los datos para el cumplimiento de sus funciones relativas a la prevención de tales delitos, en la forma prevista en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Artículo 8. *Nivel de seguridad aplicable.*

Todos los ficheros que integran la base de datos objeto de esta Ley están sometidos al nivel de seguridad alto, de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 9. *Cancelación, rectificación y acceso a los datos.*

1. La conservación de los identificadores obtenidos a partir del ADN en la base de datos objeto de esta Ley no superará:

El tiempo señalado en la ley para la prescripción del delito.

El tiempo señalado en la ley para la cancelación de antecedentes penales, si se hubiese dictado sentencia condenatoria firme, o absolutoria por la concurrencia de causas eximentes por falta de imputabilidad o culpabilidad, salvo resolución judicial en contrario.

En todo caso se procederá a su cancelación cuando se hubiese dictado auto de sobreseimiento libre o sentencia absolutoria por causas distintas de las mencionadas en el epígrafe anterior, una vez que sean firmes dichas resoluciones. En el caso de sospechosos no imputados, la cancelación de los identificadores inscritos se producirá transcurrido el tiempo señalado en la Ley para la prescripción del delito.

En los supuestos en que en la base de datos existiesen diversas inscripciones de una misma persona, correspondientes a diversos delitos, los datos y patrones identificativos inscritos se mantendrán hasta que finalice el plazo de cancelación más amplio.

2. Los datos pertenecientes a personas fallecidas se cancelarán una vez el encargado de la base de datos tenga conocimiento del fallecimiento. En los supuestos contemplados en el artículo 3.1 b), los datos inscritos no se cancelarán mientras sean necesarios para la finalización de los correspondientes procedimientos.

3. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con la base de datos policial de identificadores obtenidos a partir del ADN se podrá efectuar en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. Los identificadores obtenidos a partir del ADN respecto de los que se desconozca la identidad de la persona a la que corresponden, permanecerán inscritos en tanto se mantenga dicho anonimato. Una vez identificados, se aplicará lo dispuesto en este artículo a efectos de su cancelación.

Disposición Adicional Primera. *Integración de ficheros y bases de datos.*

1. El Ministerio del Interior adoptará las medidas oportunas para que los diferentes ficheros y bases de datos de identificadores obtenidos a partir del ADN que, en el ámbito de las Fuerzas y Cuerpos de Seguridad del Estado existieran a la entrada en vigor de esta Ley, pasen a integrarse en la base de datos policial creada por la misma.

2. Igualmente, y mediante la suscripción del oportuno convenio, será posible la integración en la nueva base de datos de los datos procedentes de otros ficheros, registros o bases de datos de identificadores obtenidos a partir del ADN, distintos a los descritos en el artículo 1 de esta Ley, siempre que los mismos hubieran sido creados con las únicas finalidades de investigación y averiguación de los delitos a los que se refiere el artículo 3.1.a) de esta Ley, identificación de cadáveres o averiguación de personas desaparecidas.

Disposición Adicional Segunda. *Régimen jurídico.*

La presente Ley se inscribe en el marco de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual, por su propia naturaleza, resulta de aplicación directa, siendo los preceptos de esta Ley especificidades habilitadas por la citada Ley Orgánica en función de la naturaleza de la base de datos que se regula.

Disposición Adicional Tercera. *Obtención de muestras biológicas.*

Para la investigación de los delitos enumerados en la letra a) del apartado 1 del artículo 3, la policía judicial procederá a la toma de muestras y fluidos del sospechoso, detenido o imputado, así como del lugar del delito. La toma de muestras que requieran inspecciones, reconocimientos o intervenciones corporales, sin consentimiento del afectado, requerirá en todo caso autorización judicial mediante auto motivado, de acuerdo con lo establecido en la Ley de Enjuiciamiento Criminal.

Disposición Adicional Cuarta. *Laboratorios del Instituto Nacional de Toxicología y Ciencias Forenses.*

A los efectos de lo dispuesto en el artículo 5 de esta Ley, los laboratorios del Instituto Nacional de Toxicología y Ciencias Forenses podrán realizar los correspondientes análisis del ADN para identificación genética, de acuerdo con las funciones que le atribuye la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Disposición Transitoria Única. *Laboratorios no acreditados.*

Los laboratorios de las Fuerzas y Cuerpos de Seguridad del Estado que a la entrada en vigor de esta Ley no estuviesen debidamente acreditados en la forma prevista en el artículo 5, dispondrán del plazo de un año para hacerlo, a contar desde dicha fecha.

Disposición Derogatoria Única. *Derogación normativa.*

Quedan derogadas cuantas normas de igual o inferior rango contradigan o se opongan a lo dispuesto en la presente Ley.

Disposición Final Primera. *Título competencial.*

La presente Ley se dicta al amparo de las reglas 1.ª, 6.ª y 29.ª del artículo 149.1 de la Constitución.

Disposición Final Segunda. *Preceptos con carácter de Ley ordinaria.*

Tienen el carácter de Ley ordinaria los artículos 2, apartado 2 del artículo 5, artículos 7, 8 y 9, y la Disposición adicional primera, Disposición adicional segunda, Disposición adicional cuarta, Disposición transitoria única, Disposición final primera, y Disposición final tercera.

Disposición Final Tercera. *Habilitación normativa.*

1. Se autoriza al Gobierno a dictar las normas que procedan para el desarrollo de lo dispuesto en la presente Ley.
2. Específicamente, se habilita al Gobierno para determinar el responsable del fichero y de su gestión, a los efectos previstos en la Ley 15/1999, de 13 de diciembre.

Disposición Final Cuarta. *Entrada en vigor.*

Esta Ley entrará en vigor al mes de su publicación en el Boletín Oficial del Estado.

§ 36

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos

Jefatura del Estado
«BOE» núm. 186, de 5 de agosto de 1997
Última modificación: sin modificaciones
Referencia: BOE-A-1997-17574

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

PREÁMBULO

El artículo 104.1 de la Constitución establece que las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, para cuyo cumplimiento actúan con absoluto respeto a la Constitución y al resto del ordenamiento, tal como recoge el mandato constitucional en su artículo 9.1 y la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, en su artículo 5.1.

La prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, y especialmente cuando las actuaciones perseguidas suceden en espacios abiertos al público, lleva a los miembros de las Fuerzas y Cuerpos de Seguridad al empleo de medios técnicos cada vez más sofisticados. Con estos medios, y en particular mediante el uso de sistemas de grabación de imágenes y sonidos y su posterior tratamiento, se incrementa sustancialmente el nivel de protección de los bienes y libertades de las personas.

Ahora es oportuno proceder a la regulación del uso de los medios de grabación de imágenes y sonidos que vienen siendo utilizados por la Fuerzas y Cuerpos de Seguridad, introduciendo las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública.

Las garantías que introduce la presente Ley en el uso de sistemas de grabación de imágenes y sonidos por parte de las Fuerzas y Cuerpos de Seguridad parten del establecimiento de un régimen de autorización previa para la instalación de videocámaras inspirado en el principio de proporcionalidad, en su doble versión de idoneidad e intervención mínima. La autorización se concederá por los órganos administrativos que se determinan

previo informe preceptivo, que será vinculante si es negativo, de una Comisión que presidirá el Pre sidente del Tribunal Superior de Justicia de la Comunidad Autónoma correspondiente, y en la cual la presencia de miembros dependientes de la Administración autorizante no podrá ser mayoritaria.

La Ley prevé, además de las instalaciones fijas de videocámaras, el uso de videocámaras móviles con la necesaria autorización del órgano designado al efecto, salvo en situaciones de urgencia o en las que sea imposible obtener a tiempo la autorización, en las cuales se procederá a comunicar su uso a la autoridad policial y a la Comisión. En todos los casos la Comisión será informada periódicamente del uso que se haga de las videocámaras móviles y tendrá derecho a recabar la correspondiente grabación.

Las imágenes y sonidos obtenidos por cualquiera de las maneras previstas serán destruidos en el plazo de un mes desde su captación, salvo que se relacionen con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial abierto. El público será informado de la existencia de videocámaras fijas y de la autoridad responsable y todas las personas interesadas podrán ejercer el derecho de acceso y cancelación de las imágenes en que hayan sido recogidos.

Finalmente, se dispone la inmediata puesta a disposición judicial de aquellas grabaciones en las que se haya captado la comisión de hechos que pudieran constituir ilícitos penales y, en previsión de que, por circunstancias que deberán ser justificadas, no sea posible, se establece la entrega de la grabación junto con el relato de los hechos a la autoridad judicial o al Ministerio Fiscal.

La Ley lleva a cabo modificaciones en otras leyes que, con el mismo fin de protección de la seguridad de las personas y de los bienes y garantía de los derechos y libertades, permitan dotar de mayor eficacia a las previsiones de ésta. Así, introduce modificaciones en la Ley Orgánica 9/1983, de 15 de julio, reguladora del Derecho de Reunión, y en la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, con la finalidad de atajar la violencia callejera que eventualmente se produce con ocasión del ejercicio del derecho de reunión y manifestación en lugares de tránsito público.

Corresponde al Estado, en el ejercicio de la competencia que le atribuye la Constitución (artículo 149.1.29.a) en materia de seguridad pública, la aprobación de la presente Ley que, por otra parte, en la medida en que incide en la regulación de las condiciones básicas del ejercicio de determinados derechos fundamentales, como el derecho a la propia imagen y el derecho de reunión, debe tener en su totalidad el carácter de Ley Orgánica, sin perjuicio de las competencias que correspondan a las Comunidades Autónomas en esta materia de acuerdo con lo que dispongan sus Estatutos de Autonomía.

Artículo 1. *Objeto.*

1. La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de autorización, grabación y uso de las imágenes y sonidos obtenidos conjuntamente por las videocámaras.

2. Las referencias contenidas en esta Ley a videocámaras, cámaras fijas y cámaras móviles se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta Ley.

Artículo 2. *Ámbito de aplicación.*

1. La captación, reproducción y tratamiento de imágenes y sonidos, en los términos previstos en esta Ley, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo.

2. Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Artículo 3. *Autorización de las instalaciones fijas.*

1. La instalación de videocámaras o de cualquier medio técnico análogo en los términos del artículo 1.2 de la presente Ley está sujeta al régimen de autorización, que se otorgará, en su caso, previo informe de un órgano colegiado presidido por un Magistrado y en cuya composición no serán mayoría los miembros dependientes de la Administración autorizante.

2. Las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales serán autorizadas por el Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la misma Comunidad. La composición y funcionamiento de la Comisión, así como la participación de los municipios en ella, se determinarán reglamentariamente.

3. No podrá autorizarse la instalación fija de videocámaras cuando el informe de la Comisión prevista en el apartado segundo de este artículo estime que dicha instalación supondría una vulneración de los criterios establecidos en el artículo 4 de la presente Ley Orgánica.

4. La resolución por la que se acuerde la autorización deberá ser motivada y referida en cada caso al lugar público concreto que ha de ser objeto de observación por las videocámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes. Asimismo, deberá precisar genéricamente el ámbito físico susceptible de ser grabado, el tipo de cámara, sus especificaciones técnicas y la duración de la autorización, que tendrá una vigencia máxima de un año, a cuyo término habrá de solicitarse su renovación.

5. La autorización tendrá en todo caso carácter revocable.

Artículo 4. *Criterios de autorización de instalaciones fijas.*

Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes.

Artículo 5. *Autorización de videocámaras móviles.*

1. En las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, podrán utilizarse simultáneamente otras de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6.

2. También podrán utilizarse en los restantes lugares públicos videocámaras móviles. La autorización de dicho uso corresponderá al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización del medio a los principios previstos en el artículo 6.

La resolución motivada que se dicte autorizando el uso de videocámaras móviles se pondrá en conocimiento de la Comisión prevista en el artículo 3 en el plazo máximo de setenta y dos horas, la cual podrá recabar el soporte físico de la grabación a efectos de emitir el correspondiente informe.

En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, se podrán obtener imágenes y sonidos con videocámaras

móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión aludida en el párrafo anterior, la cual, si lo estima oportuno, podrá requerir la entrega del soporte físico original y emitir el correspondiente informe.

En el supuesto de que los informes de la Comisión previstos en los dos párrafos anteriores fueran negativos, la autoridad encargada de la custodia de la grabación procederá a su destrucción inmediata.

3. La Comisión prevista en el artículo 3 será informada quincenalmente de la utilización que se haga de videocámaras móviles y podrá recabar en todo momento el soporte de las correspondientes grabaciones y emitir un informe al respecto.

4. En el caso de que las autoridades competentes aludidas en esta Ley lo consideren oportuno, se podrá interesar informe de la Comisión prevista en el artícu lo 3 sobre la adecuación de cualquier registro de imágenes y sonidos obtenidos mediante videocámaras móviles a los principios del artículo 6.

Artículo 6. *Principios de utilización de las videocámaras.*

1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.

2. La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

3. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

4. La utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artícu lo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia.

Artículo 7. *Aspectos procedimentales.*

1. Realizada la filmación de acuerdo con los requisitos establecidos en la Ley, si la grabación captara la comisión de hechos que pudieran ser constitutivos de ilícitos penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la mayor inmediatez posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si la grabación captara hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad ciudadana, se remitirán al órgano competente, igualmente de inmediato, para el inicio del oportuno procedimiento sancionador.

Artículo 8. *Conservación de las grabaciones.*

1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.

3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo.

4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados.

Artículo 9. *Derechos de los interesados.*

1. El público será informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable.

2. Toda persona interesada podrá ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura. No obstante, el ejercicio de estos derechos podrá ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Artículo 10. *Infracciones y sanciones.*

Cuando no haya lugar a exigir responsabilidades penales, las infracciones a lo dispuesto en la presente Ley serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de tratamiento automatizado de los datos de carácter personal.

Artículo 11. *Recursos.*

Contra las resoluciones dictadas en aplicación de lo previsto en esta Ley, cabrá la interposición de los recursos ordinarios en vía administrativa, contencioso-administrativa, así como los previstos en el artículo 53.2 de la Constitución, en los términos legalmente establecidos.

Disposición adicional primera.

Las Comunidades Autónomas con competencia para la protección de las personas y los bienes y para el mantenimiento del orden público, con arreglo a lo dispuesto en los correspondientes Estatutos de Autonomía, podrán dictar, con sujeción a lo prevenido en esta Ley, las disposiciones necesarias para regular y autorizar la utilización de videocámaras por sus fuerzas policiales y por las dependientes de las Corporaciones locales radicadas en su territorio, la custodia de las grabaciones obtenidas, la responsabilidad sobre su ulterior destino y las peticiones de acceso y cancelación de las mismas.

Cuando sean competentes para autorizar la utilización de videocámaras, las Comunidades Autónomas mencionadas en el párrafo anterior regularán la composición y el funcionamiento de la Comisión correspondiente, prevista en el artículo 3 de esta Ley, con especial sujeción a los principios de presidencia judicial y prohibición de mayoría de la Administración autorizante.

Disposición adicional segunda.

Cada autoridad competente para autorizar la instalación fija de videocámaras por parte de las Fuerzas y Cuerpos de Seguridad deberá crear un registro en el que consten todas las que haya autorizado.

Disposición adicional tercera.

El artículo 4.3 de la Ley Orgánica 9/1983, de 15 de julio, Reguladora del Derecho de Reunión, queda redactado de la siguiente forma:

«3. Los participantes en reuniones o manifestaciones, que causen un daño a terceros, responderán directamente de él. Subsidiariamente, las personas naturales o jurídicas

organizadoras o promotoras de reuniones o manifestaciones responderán de los daños que los participantes causen a terceros, sin perjuicio de que puedan repetir contra aquéllos, a menos que hayan puesto todos los medios razonables a su alcance para evitarlos.»

Disposición adicional cuarta.

1. Se da nueva redacción al artículo 23.c) de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, que queda redactado de la siguiente forma:

> «c) La celebración de reuniones en lugares de tránsito público o de manifestaciones, incumpliendo lo preceptuado en los artículos 4.2, 8, 9, 10 y 11 de la Ley Orgánica 9/1983, de 15 de julio, Reguladora del Derecho de Reunión, cuya responsabilidad corresponde a los organizadores o promotores, siempre que tales conductas no sean constitutivas de infracción penal.
>
> En el caso de reuniones en lugares de tránsito público y manifestaciones cuya celebración se haya comunicado previamente a la autoridad se considerarán organizadores o promotores las personas físicas o jurídicas que suscriban el correspondiente escrito de comunicación.
>
> Aun no habiendo suscrito o presentado la citada comunicación, también se considerarán organizadores o promotores, a los efectos de esta Ley, a quienes de hecho las presidan, dirijan o ejerzan actos semejantes o a quienes por publicaciones o declaraciones de convocatoria de las reuniones o manifestaciones, por los discursos que se pronuncien y los impresos que se repartan durante las mismas, por los lemas, banderas u otros signos que ostenten o por cualesquiera otros hechos, pueda determinarse razonablemente que son inspiradores de aquéllas.»

2. Se da nueva redacción al artículo 23.d) de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, que queda redactado como sigue:

> «d) La negativa a disolver las manifestaciones y reuniones en lugares de tránsito público ordenada por la autoridad competente cuando concurran los supuestos del artículo 5 de la Ley Orgánica 9/1983.»

3. Los actuales párrafos d), e), f), g), h), i), j), k), l), m), n) y ñ) del artículo 23 de la Ley Orgánica citada se convertirán en los párrafos e), f), g), h), i), j), k), l), m), n), ñ) y o), respectivamente.

Disposición adicional quinta.

Las autorizaciones de instalaciones fijas de videocámaras constituyen actividades de protección de la seguridad pública realizadas al amparo del artículo 149.1.29.a de la Constitución y no estarán sujetas al control preventivo de las Corporaciones locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa.

Disposición adicional sexta.

Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por las instalaciones reguladas en esta Ley, o quienes los posean por cualquier título, están obligados a facilitar y permitir su colocación y mantenimiento, sin perjuicio de la necesidad de obtener, en su caso, la autorización judicial prevista en el artículo 87.2 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y de las indemnizaciones que procedan según las leyes.

Disposición adicional séptima.

1. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

a) Alterar o manipular los registros de imágenes y sonidos siempre que no constituya delito.

b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar éstos para fines distintos de los previstos legalmente.

c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley.

d) Utilizar los medios técnicos regulados en esta Ley para fines distintos de los previstos en la misma.

2. Se considerarán faltas graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado las restantes infracciones a lo dispuesto en la presente Ley.

Disposición adicional octava.

La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto ar ticulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia, y con sujeción a lo dispuesto en las Leyes Orgánicas 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, en el marco de los principios de utilización de las mismas previstos en esta Ley.

Disposición adicional novena.

El Gobierno elaborará, en el plazo de un año, la normativa correspondiente para adaptar los principios inspiradores de la presente Ley al ámbito de la seguridad privada.

Disposición transitoria única.

En el plazo de seis meses a partir de la entrada en vigor de la presente Ley, se procederá, en su caso, a autorizar las instalaciones fijas de videocámaras actualmente existentes, así como a destruir aquellas grabaciones que no reúnan las condiciones legales para su conservación.

Disposición final primera.

El Gobierno, en el plazo de seis meses desde la entrada en vigor de esta Ley, aprobará las disposiciones reglamentarias necesarias para su ejecución y desarrollo.

Disposición final segunda.

Esta Ley entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

§ 37

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 77, de 31 de marzo de 2015
Última modificación: 23 de febrero de 2021
Referencia: BOE-A-2015-3442

[. . .]

CAPÍTULO II

Documentación e identificación personal

Artículo 8. *Acreditación de la identidad de los ciudadanos españoles.*

1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.

2. En el Documento Nacional de Identidad figurarán la fotografía y la firma de su titular, así como los datos personales que se determinen reglamentariamente, que respetarán el derecho a la intimidad de la persona, sin que en ningún caso, puedan ser relativos a la raza, etnia, religión, creencias, opinión, ideología, discapacidad, orientación o identidad sexual, o afiliación política o sindical. La tarjeta soporte del Documento Nacional de Identidad incorporará las medidas de seguridad necesarias para la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación.

3. El Documento Nacional de Identidad permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica. Las personas con capacidad modificada judicialmente podrán ejercer esas facultades cuando expresamente lo solicite el interesado y no precise, atendiendo a la resolución judicial que complemente su capacidad, de la representación o asistencia de una institución de protección y apoyo para obligarse o contratar.

El prestador de servicios de certificación procederá a revocar el certificado de firma electrónica a instancia del Ministerio del Interior, tras recibir éste la comunicación del Encargado del Registro Civil de la inscripción de la resolución judicial que determine la necesidad del complemento de la capacidad para obligarse o contratar, del fallecimiento o de la declaración de ausencia o fallecimiento de una persona.

[. . .]

CAPÍTULO III

Actuaciones para el mantenimiento y restablecimiento de la seguridad ciudadana

Sección 1.ª Potestades generales de policía de seguridad

[. . .]

Artículo 16. *Identificación de personas.*

1. En el cumplimiento de sus funciones de indagación y prevención delictiva, así como para la sanción de infracciones penales y administrativas, los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas en los siguientes supuestos:

a) Cuando existan indicios de que han podido participar en la comisión de una infracción.
b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito.

En estos supuestos, los agentes podrán realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados.

En la práctica de la identificación se respetarán estrictamente los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social.

2. Cuando no fuera posible la identificación por cualquier medio, incluida la vía telemática o telefónica, o si la persona se negase a identificarse, los agentes, para impedir la comisión de un delito o al objeto de sancionar una infracción, podrán requerir a quienes no pudieran ser identificados a que les acompañen a las dependencias policiales más próximas en las que se disponga de los medios adecuados para la práctica de esta diligencia, a los solos efectos de su identificación y por el tiempo estrictamente necesario, que en ningún caso podrá superar las seis horas.

La persona a la que se solicite que se identifique será informada de modo inmediato y comprensible de las razones de dicha solicitud, así como, en su caso, del requerimiento para que acompañe a los agentes a las dependencias policiales.

3. En las dependencias a que se hace referencia en el apartado 2 se llevará un libro-registro en el que sólo se practicarán asientos relacionados con la seguridad ciudadana. Constarán en él las diligencias de identificación practicadas, así como los motivos, circunstancias y duración de las mismas, y sólo podrán ser comunicados sus datos a la autoridad judicial competente y al Ministerio Fiscal. El órgano competente de la Administración remitirá mensualmente al Ministerio Fiscal extracto de las diligencias de identificación con expresión del tiempo utilizado en cada una. Los asientos de este libro-registro se cancelarán de oficio a los tres años.

4. A las personas desplazadas a dependencias policiales a efectos de identificación, se les deberá expedir a su salida un volante acreditativo del tiempo de permanencia en ellas, la causa y la identidad de los agentes actuantes.

5. En los casos de resistencia o negativa a identificarse o a colaborar en las comprobaciones o prácticas de identificación, se estará a lo dispuesto en el Código Penal, en la Ley de Enjuiciamiento Criminal y, en su caso, en esta Ley.

Artículo 17. *Restricción del tránsito y controles en las vías públicas.*

1. Los agentes de las Fuerzas y Cuerpos de Seguridad podrán limitar o restringir la circulación o permanencia en vías o lugares públicos y establecer zonas de seguridad en supuestos de alteración de la seguridad ciudadana o de la pacífica convivencia, o cuando

existan indicios racionales de que pueda producirse dicha alteración, por el tiempo imprescindible para su mantenimiento o restablecimiento. Asimismo podrán ocupar preventivamente los efectos o instrumentos susceptibles de ser utilizados para acciones ilegales, dándoles el destino que legalmente proceda.

2. Para la prevención de delitos de especial gravedad o generadores de alarma social, así como para el descubrimiento y detención de quienes hubieran participado en su comisión y proceder a la recogida de los instrumentos, efectos o pruebas, se podrán establecer controles en las vías, lugares o establecimientos públicos, siempre que resulte indispensable proceder a la identificación de personas que se encuentren en ellos, al registro de vehículos o al control superficial de efectos personales.

[. . .]

CAPÍTULO IV

Potestades especiales de policía administrativa de seguridad

Artículo 25. *Obligaciones de registro documental.*

1. Las personas físicas o jurídicas que ejerzan actividades relevantes para la seguridad ciudadana, como las de hospedaje, transporte de personas, acceso comercial a servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público, comercio o reparación de objetos usados, alquiler o desguace de vehículos de motor, compraventa de joyas y metales, ya sean preciosos o no, objetos u obras de arte, cerrajería de seguridad, centros gestores de residuos metálicos, establecimientos de comercio al por mayor de chatarra o productos de desecho, o de venta de productos químicos peligrosos a particulares, quedarán sujetas a las obligaciones de registro documental e información en los términos que establezcan las disposiciones aplicables.

2. Los titulares de embarcaciones de alta velocidad, así como los de aeronaves ligeras estarán obligados a realizar las actuaciones de registro documental e información previstas en la normativa vigente.

[. . .]

§ 38

Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas. [Inclusión parcial]

Ministerio del Interior
«BOE» núm. 55, de 5 de marzo de 1993
Última modificación: 5 de agosto de 2020
Referencia: BOE-A-1993-6202

[. . .]

CAPÍTULO PRELIMINAR

Disposiciones generales

[. . .]

Artículo 10.

1. Para el ejercicio de la actividad de armero en cualquiera de sus modalidades, se requerirá la obtención de una autorización previa expedida por la Dirección General de la Guardia Civil, sobre la base de la comprobación de la integridad privada y profesional, la competencia en la materia y la carencia de antecedentes penales por delito doloso del solicitante, así como la acreditación de las aptitudes psicofísicas necesarias salvo que, en cuanto a esto último, el solicitante fuese titular de una licencia de armas.

2. Cuando se trate de personas jurídicas, el control se llevará a cabo, tanto sobre la persona jurídica, como sobre la persona o las personas físicas que dirijan la empresa.

3. Para el ejercicio de la actividad de corredor se requerirá la obtención de una autorización previa expedida por la Dirección General de la Guardia Civil, a la que será de aplicación lo establecido en los apartados anteriores para la obtención de la autorización de armero.

4. Durante su período de actividad, los armeros y los corredores estarán obligados a mantener un registro en el que consignarán, en los casos previstos en este Reglamento, las armas y los componentes esenciales a los que den entrada y salida, con los datos que permitan la identificación y la localización del arma o del componente esencial de que se trate, en particular, el tipo, la marca, el modelo, el calibre y el número de fabricación, así como el nombre, la dirección, la nacionalidad, y los demás datos de identificación necesarios del proveedor y del adquirente. Las Intervenciones de Armas y Explosivos de la Guardia Civil comprobarán periódicamente el cumplimiento de esta obligación por parte de los armeros y corredores. Los armeros y los corredores, tras el cese de su actividad, entregarán dichos registros a la Intervención de Armas y Explosivos correspondiente al lugar donde radique el establecimiento.

5. Los armeros y corredores comunicarán a la Intervención de Armas y Explosivos, sin demora indebida y por medios electrónicos, informáticos o telemáticos, las transacciones de las armas de fuego y asimiladas, sus componentes esenciales, armas de alarma y señales, armas acústicas y de salvas e inutilizadas, al objeto de su grabación inmediata en el Registro Nacional de Armas.

6. Los armeros y los corredores podrán negarse a efectuar cualquier transacción de adquisición de armas, componentes esenciales, munición o componentes de esta, que razonablemente consideren sospechosa debido a su naturaleza o magnitud, e informarán de cualquier intento de realizar dicha transacción a la Intervención de Armas y Explosivos correspondiente.

7. La Dirección General de la Guardia Civil dispondrá de un registro de los armeros y corredores que operen en el territorio nacional. El tratamiento de los datos de carácter personal se realizará de conformidad con la normativa reguladora que le sea de aplicación.

8. Las actividades relacionadas con la fabricación, comercio y distribución de armas, componentes esenciales y sus municiones, constituyen un sector con regulación específica en materia de derecho de establecimiento, en los términos previstos por la legislación sobre inversiones extranjeras en España, correspondiendo a los Ministerios de Defensa, del Interior y de Industria, Comercio y Turismo el ejercicio de las competencias de supervisión y control.

Las inversiones extranjeras, directas o indirectas, en sociedades españolas que tengan por objeto desarrollar las actividades indicadas se ajustarán a los requisitos y condiciones establecidas en el Real Decreto 664/1999, de 23 de abril, sobre inversiones exteriores.

[. . .]

CAPÍTULO III

Medidas de seguridad en fabricación, circulación y comercio

[. . .]

Artículo 87.

1. Las cajas fuertes a que hace referencia el artículo anterior deberán ser puntos activos de las señales de alarma.

2. Si las condiciones de seguridad de estas cajas fuertes no fuesen suficientes, la Intervención de Armas de la Guardia Civil podrá disponer que sean depositados en ella o en el lugar adecuado que designe las piezas o elementos esenciales separados.

[. . .]

CAPÍTULO V

Licencias, autorizaciones especiales y tarjetas de armas

Sección 1. Licencias en general y tarjetas

[. . .]

Aptitudes físicas y psíquicas

Artículo 98.

1. En ningún caso podrán tener ni usar armas, ni ser titulares de las licencias o autorizaciones correspondientes, las personas cuyas condiciones psíquicas o físicas les impidan su utilización, y especialmente aquellas personas para las que la posesión y el uso de armas representen un riesgo propio o ajeno, la seguridad pública, la seguridad ciudadana, la defensa nacional y el interés general. Entre otros extremos, el hecho de haber tenido una condena por un delito doloso violento se considerará indicativo de dicho riesgo.

2. Para solicitar las licencias y autorizaciones especiales de armas, además de la documentación requerida para cada supuesto en los correspondientes artículos de este Reglamento, los interesados deberán acreditar la posesión de las aptitudes psíquicas y físicas adecuadas y los conocimientos necesarios sobre conservación, mantenimiento y manejo de las armas, en la forma prevenida.

3. La acreditación de las aptitudes psíquicas y físicas necesarias para poder obtener la concesión, así como la renovación de licencias y autorizaciones especiales para la tenencia y uso de armas, deberá llevarse a cabo mediante la presentación, ante las oficinas instructoras de los procedimientos, del correspondiente informe de aptitud.

4. De lo dispuesto en el apartado anterior se exceptúa el personal que se encuentre en activo o en la situación que se estime reglamentariamente como tal, de las Fuerzas Armadas y de las Fuerzas y Cuerpos de Seguridad.

Expedición de licencias B, D y E a particulares

Artículo 99.

1. La licencia de armas B solamente podrá ser expedida a quienes tengan necesidad de obtenerla, y será competente para concederla la Dirección General de la Guardia Civil.

2. En la solicitud o en memoria adjunta se harán constar con todo detalle los motivos que fundamenten la necesidad de la posesión de arma corta, acompañando a aquélla cuantos documentos desee aportar el solicitante, que sirvan para fundamentar la necesidad de usar el arma, teniendo en cuenta que la razón de defensa de personas o bienes, por sí sola, no justifica la concesión de la licencia, cuya expedición tendrá carácter restrictivo, limitándose a supuestos de existencia de riesgo especial y de necesidad.

3. La oficina receptora, con su informe, dará curso a la solicitud ; el Jefe de la Comandancia de la Guardia Civil, con el suyo, la remitirá al Gobernador civil de la provincia.

4. El Gobernador civil, a la vista de los datos y los antecedentes aportados, emitirá su informe que, junto a la preceptiva documentación, enviará a la Dirección General de la Guardia Civil.

5. La Dirección General de la Guardia Civil, en el caso de que sea favorable el informe del Gobierno Civil, valorando objetivamente los antecedentes, hechos y criterios aportados, y previas las comprobaciones pertinentes, concederá la licencia o la denegará motivadamente, según las circunstancias de cada caso.

6. Estas licencias tendrán cinco años de validez, al cabo de los cuales, para poder usar las armas autorizadas con ellas, habrán de solicitarse nuevas licencias en la misma forma que las anteriores. Nadie podrá poseer más de una licencia B, y cada licencia no amparará más de un arma.

7. El arma será guardada en los propios domicilios de sus titulares en un lugar seguro bajo llave separada de su munición, de forma que no sean fácilmente accesibles de manera conjunta.

[. . .]

Tarjetas

Artículo 105.

1. Para poder llevar y usar las armas de la categoría 4.ª fuera del domicilio habrán de estar documentadas singularmente, mediante tarjetas de armas, que las acompañarán en todo caso.

Las tarjetas de armas serán concedidas y retiradas, en su caso, por los Alcaldes de los municipios en que se encuentren avecindados o residiendo los solicitantes, previa consideración de la conducta y antecedentes de los mismos. Su validez quedará limitada a los respectivos términos municipales.

2. Las armas incluidas en la categoría 4.ª, 2, se pueden documentar en número ilimitado con tarjeta B, cuya validez será permanente. De las comprendidas en la categoría 4.ª, 1, solamente se podrán documentar seis armas con tarjetas A cuya validez será de cinco años.

3. No obstante, la autoridad municipal podrá limitar o reducir, tanto el número de armas que puede poseer cada interesado como el tiempo de validez de las tarjetas, teniendo en cuenta las circunstancias locales y personales que concurran.

4. Los solicitantes de la tarjeta A deberán acreditar haber cumplido catorce años de edad, a cuyo efecto habrán de presentar documento nacional de identidad o documentos equivalentes en vigor.

5. La tarjeta de armas se expedirá en impreso, que confeccionará la Dirección General de la Guardia Civil.

En cada impreso se podrán reseñar hasta seis armas. Cuando se trate de tarjetas B y el número de armas exceda de seis, el interesado podrá ser titular de más de una tarjeta.

6. Del impreso se destinará un ejemplar al interesado ; el segundo será remitido por la Alcaldía a la Intervención de Armas.

[. . .]

Armas antiguas, históricas y artísticas. Armas de avancarga y de sistema «Flobert». Armas acústicas y de salvas. Armas inutilizadas

[. . .]

Artículo 109.

1. Los españoles y extranjeros, con residencia en España, que sean mayores de dieciséis años y menores de dieciocho, podrán utilizar exclusivamente para la caza o para el tiro deportivo en cuyos Reglamentos se halle reconocida la categoría ‘‘junior’’, pero no poseer ni llevar dentro de las poblaciones, armas largas rayadas para caza mayor o, en su caso, de la categoría 3.ª 1, siempre que se encuentren en posesión legal de una autorización especial de uso de armas para menores y estén sometidos a la supervisión de un adulto titular de licencia de armas D, E o F, que previamente se hayan comprometido a acompañarlos y vigilarlos en cada cacería o acto deportivo, y asuman la responsabilidad de su adecuado almacenamiento de conformidad con los artículos 100.5, 101.5 y 133.2.

2. Con las mismas condiciones y requisitos, los mayores de catorce años y menores de dieciocho podrán utilizar las armas de la categoría 3.ª, 2, para la caza y las de la categoría 3.ª, 2 y 3, para competiciones deportivas en cuyos Reglamentos se halle reconocida la categoría «junior», obteniendo una autorización especial de uso de armas para menores.

3. Las autorizaciones especiales de uso de armas para menores tendrán validez hasta la mayoría de edad de sus titulares, sin necesidad de obtener renovaciones, y será competente para concederlas el Director general de la Guardia Civil.

4. Las solicitudes se presentarán en las Comandancias o Puestos de la Guardia Civil correspondientes al domicilio del interesado suscritas por éste y por la persona que ejerce la patria potestad o la tutela sobre el mismo, y habrán de acompañarse los documentos siguientes:

a) Certificado de antecedentes penales, si se trata de mayores de dieciséis años.

b) Certificado de antecedentes penales de la persona que ejerza la patria potestad o la tutela sobre el solicitante.

c) Fotocopias de los documentos nacionales de identidad en vigor de ambos, o de las tarjetas o autorizaciones de residencia si se trata de extranjeros, que serán cotejadas con sus originales, devolviéndose éstos a los interesados.

d) Autorización para el uso de armas de las clases expresadas, otorgada por la persona que ejerza la patria potestad o la tutela, responsabilizándose de su actuación, ante Notario, autoridad gubernativa, alcaldía, Comisaría de Policía, Comandancia, Intervención de Armas o Puesto de la Guardia Civil.

e) Informe de aptitudes psicofísicas.

No será necesaria la presentación de los documentos reseñados, relativos a la persona que ejerza la patria potestad o la tutela, si ésta se encuentra en posesión de cualquier licencia de armas en vigor.

5. Las solicitudes y los documentos señalados habrán de ser remitidos a la Dirección General de la Guardia Civil, acompañándose informe de conducta y antecendentes del interesado y de la persona que ejerza la patria potestad o la tutela.

[. . .]

CAPÍTULO VI

Tenencia y uso de armas de concurso

[. . .]

Artículo 131.

La Dirección General de la Guardia Civil, valorando objetivamente los antecedentes y hechos aportados, y previas las comprobaciones pertinentes, concederá o no la licencia, según las circunstancias de cada caso, y la remitirá a la Intervención de Armas correspondiente, para su entrega al interesado.

[. . .]

INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 1

Características y medidas de seguridad en galerías y campos de tiro.

A) GALERÍAS DE TIRO

Especificaciones

1. Puestos de tirador

a) Espacio para el tirador.

El tirador debe disponer de un espacio comprendido entre 1 y 1,5 metros de ancho, con una profundidad de 1,3 a 1,5 metros, según modalidades de tiro y calibre de las armas empleadas.

b) Pantallas de separación de tiradores.

Deben colocarse pantallas para separar los diversos puestos de tiro en evitación de accidentes debidos a la expulsión de los casquillos; sus dimensiones serán: Altura mínima, 2 metros; anchura, 1,5 metros; altura del suelo, menos de 0,70 metros.

c) Protección con marquesinas.

Tiene por misión la limitación del ángulo de tiro, siendo sus medidas ideales: Altura del extremo más bajo, 2 metros; longitud, de 2,5 a 3 metros, limitando el ángulo de tiro a 40 grados para evitar la excesiva altura del primer parabalas. Deben estar protegidas contra la penetración de la munición empleada. Pueden ser de:

1. Hormigón recubierto con madera para evitar rebotes.
2. Madera de 4 centímetros de espesor, como mínimo, más una chapa de hierro de 2 milímetros, si solo se emplea 22. Si se emplea otra munición, ver tabla de penetraciones adjunta.

d) Protección de cristaleras.

Deben estar fuera de la línea de tiro. De prever posibilidad de impacto serán antibala del espesor adecuado a la munición a emplear, ver tabla adjunta de cristales de seguridad.

e) Piso adecuado.

El piso debe ser plano, horizontal en todas las direcciones y rugoso para evitar deslizamientos, ya que un resbalón del tirador puede provocar un disparo fortuito.

f) Mesa para colocar el arma y la munición.

Cada tirador dispondrá de una mesa situada en la parte delantera del puesto de tirador para colocar el arma y la munición. Sus dimensiones serán de unos 50 por 50 centímetros y una altura de 70 a 100 centímetros. Su objeto es que el arma allí depositada siempre esté con el cañón hacia el campo de tiro.

g) Puertas de acceso directo.

No es recomendable que existan puertas que abran directamente a la sala de tirador que puedan cerrarse violentamente, pues el ruido que producen puede dar lugar a un disparo involuntario.

h) Iluminación adecuada.

Es recomendable luz cenital natural o artificial con difusores para no producir deslumbramientos o brillos molestos para el tirador.

i) Insonorización.

Es muy conveniente, sobre todo en aquellas galerías completamente cerradas, pues la reverberación que producen los disparos, pese a usar normalmente cascos, puede producir disparos fortuitos. A título de ejemplo, una buena insonorización puede conseguirse con 100 milímetros de planchas de fibra de vidrio recubiertas con panel perforado.

j) Caja fuerte o cámara acorazada.

Han de tenerla todas aquellas galerías en que queden depositadas armas y municiones, antes o después de las tiradas.

2. Parabalas

Son aquellas pantallas que se colocan a lo largo del campo de tiro y deben interceptar con toda seguridad cualquier trayectoria que trate de salirse de los límites del campo.

a) Espesor de acuerdo con la munición empleada.

Lo ideal es que sean de hormigón armado de 20 centímetros, cubierto siempre con madera por la parte del impacto para evitar los rebotes. Pueden hacerse también de:

1. Bovedilla rellena de arcilla o arena, recubiertas de madera cuando no se emplea munición superior al 38 con bala no blindada.
2. No es recomendable parabalas solamente de madera, aunque su espesor sea el adecuado a la munición, ya que se deterioran fácilmente perdiendo su eficacia.
3. En caso de duda pueden completarse con una chapa de hierro.

b) Altura adecuada con margen de seguridad.

La altura deberá ser tal, que la trayectoria más desfavorable (normalmente es la de posición tendido, si se practica esa modalidad) deberá incidir en un parabalas con un margen de seguridad al menos de 50 centímetros del borde superior. Cuando los parabalas no cubran las trayectorias desde la posición de tendido, por no practicarse esta modalidad, es muy conveniente colocar un muro de ladrillo separando los puestos de tirador del campo de tiro y de una altura tal que corte cualquier trayectoria que desde el suelo pueda salirse del campo.

c) Número y altura de acuerdo con paramentos laterales.

1. Los parabalas deben estar distribuidos a lo largo del campo de tal forma, que una trayectoria tangente a cualquiera de ellos por su parte inferior, deberá incidir en el siguiente con un margen de seguridad de 50 centímetros.
Su número depende mucho de las condiciones particulares de cada campo, así como de la altura de la marquesina y la situación del primer parabalas, ya que estos dos elementos limitan los posibles ángulos de tiro.
Su anchura será la de la galería y soportada por el menor número de pilares posible.
2. A título orientativo, si el primer parabalas está entre 8 y 10 metros, será suficiente:

Galería de 25 metros: De 1 a 2 parabalas.

Galería de 50 metros: De 2 a 3 parabalas.
Galería de 100 metros: De 3 a 4 parabalas.
Galería de 200 metros: De 5 a 6 parabalas.

d) Altura y contextura de paramentos laterales.

1. Los paramentos laterales deben tener una altura tal que eviten la salida lateral de las balas del campo y que alguna bala al rebotar sobre ellos se salga por el parámetro opuesto.
2. Su construcción y la situación de accesos deben ser tales que impidan con seguridad la entrada de personal al campo durante las tiradas.
3. Si son hechos de desmonte, estarán cubiertos de tierra blanda plantada con césped y plantas que sujeten la tierra.
4. Si son de obra de fábrica, deberán preverse los posibles rebotes, cubriendo con madera, al menos, su última parte. Se supone que una bala de plomo puede rebotar cuando incide con un ángulo menor de 20 grados.
5. Su espesor estará de acuerdo con la munición a emplear.
6. Deben preverse los rebotes que puedan salirse fuera de los límites del campo. Para ello:

Los parabalas en altura estarán protegidos con madera por la parte de los impactos.
Los paramentos laterales estarán protegidos con madera, al menos, en las partes en que se prevé que los rebotes puedan salirse del campo.
Para evitar los rebotes sobre el suelo, deberá tener, uniformemente repartidos, promontorios de tierra de 0,50 metros de alto por 0,50 metros de ancho, con una longitud análoga a la anchura del campo, plantados de césped para evitar su desmoronamiento.

e) Protección de columnas.

Los parabalas, marquesinas de blancos, etc., deberán tener el mínimo número de columnas que su construcción permita.
En caso de que existiesen:

1. Serán cuadradas, nunca redondas ni con bordes redondeados, y colocadas de tal forma que los impactos incidan sobre superficies planas perpendiculares a la línea de tiro.
2. Estarán siempre protegidas con madera para evitar rebotes.
3. No se permitirá ningún tipo de tirante metálico de sujeción de los elementos del campo en los que pueda incidir y desviar algún disparo.

f) Mantenimiento de las protecciones contra los rebotes.

Las protecciones de madera, suelen deteriorarse rápidamente, bien por efecto de los disparos, bien debido a las inclemencias del tiempo, perdiendo su eficacia como protección.

1. Se deben proteger con tejadillos siempre que sea posible.
2. Se deben colocar de forma que su reposición sea fácil.

3. Espaldones

Son aquellos elementos destinados a detener los proyectiles disparados en el campo o galería de tiro y pueden ser:

1. Naturales, aprovechando la configuración del terreno.
2. De tierra en talud a 45 grados.
3. De muro con tierra en talud de 45 grados.
4. De muro con recubrimiento de troncos.

a) Anchura.

Necesariamente deben cubrir todo el ancho de la galería.

b) Altura mínima. La altura mínima exigida es:

1. Si es natural o fabricado con tierra amontonada formando un doble talud, su altura deberá sobrepasar 1,50 a 2 metros la trayectoria más desfavorable.

2. Si es de muro con tierra en talud, éste deberá sobrepasar 0,50 metros la trayectoria más desfavorable y el muro de contención que sobresalga de esta altura estará cubierto de madera.

c) Relación con la penetración de las armas.

1. Si es de tierra, la trayectoria más desfavorable deberá tener un recorrido de detención de al menos 1,5 metros.
2. Si es de muro con tierra en talud, el muro será de un espesor tal que por sí solo pueda detener un impacto del máximo calibre que se emplee.
3. Si es de muro recubierto de troncos, habrá que calcularlo con un gran margen de seguridad ya que la madera se deteriora muy rápidamente, sobre todo en la línea de dianas; siendo un buen complemento, en caso de duda, proteger el muro en esa zona con una chapa de hierro de 5 a 10 milímetros.

A título orientativo, una bala de 7,62 milímetros a 83 m/s, requiere un espaldón de hormigón de 24 centímetros, contando el margen de seguridad.

d) Espaldones hechos con materiales que producen rebotes.

1. Los taludes de tierra deberán estar recubiertos de tierra vegetal desprovista de piedras.
2. Los muros de contención que sobresalgan del talud, deberán cubrirse con madera. Es un buen complemento terminar el muro en una cornisa que evita la salida de algún rebote o guijarro de la tierra proyectado por el impacto.

e) Desmoronamiento producido por las inclemencias del tiempo.

Si es de tierra en doble talud, tendrá en su parte superior una zona plana de al menos 0,5 metros. En cualquier caso, todos los hechos con tierra, estarán recubiertos con césped o plantas de raíces largas que sujeten la tierra.

f) Protección del paso de personas.

Debe protegerse con toda seguridad el paso de personas a través del espaldón.

1. Si es de doble talud, tendrá un cerramiento por su parte trasera, bien de fábrica, bien de tela metálica. Se suele plantar la parte trasera del espaldón con plantas espinosas que a la par que sujetan la tierra, tienen un efecto disuasorio adicional.
2. Si tiene muro de contención, su altura por la parte trasera deberá ser como mínimo de 2,5 metros sobre el terreno.

4. Línea de blancos

a) Protección de los sirvientes.

1. Su construcción deberá ser subterránea, de hormigón, de un espesor mínimo de 10 centímetros. Es muy conveniente que tenga un voladizo de 70 a 80 centímetros que lo cubra parcialmente.
2. La parte del foso en la dirección del espaldón puede ser de tierra con inclinación natural, o de hormigón, y ha de cumplir las siguientes condiciones:

1. Nunca hará de espaldón que deberá estar como mínimo a 5 metros.
2. Su altura no será superior a la pared más próxima a los puestos de tirador.
3. Las dimensiones serán: Altura superior a 2 metros y ancho de 1,5 a 2 metros.

b) Protección contra rebotes.

Deberá colocarse un talud de tierra de aproximadamente 1 metro de alto que proteja el techo del foso de blancos de los impactos y eviten el rebote, a la par que cubra las trayectorias que incidan sobre las partes metálicas de los soportes de blancos.
La pared más próxima a los blancos será más baja o como máximo de la misma altura que la más próxima a los puestos de tirador, precisamente para que ningún impacto pueda incidir sobre ella y dañar a los sirvientes.

c) Acceso seguro.

Los fosos de tirador deben ocupar todo el ancho de la galería y su acceso deberá ser subterráneo y lateral por fuera del límite de los paramentos laterales.

Si estas dos soluciones no fueran posibles, deberá tener ineludiblemente un sistema eléctrico fiable de señales luminosas o acústicas, que no permita el tiro cuando hay personas en el campo.

5. Instalación eléctrica

Aunque una instalación eléctrica mal protegida no afecta directamente a la seguridad de las personas, sí indirectamente, ya que un cortocircuito motivado por un disparo puede dar lugar a algún disparo fortuito de los tiradores. Por tanto, toda la instalación eléctrica deberá ser subterránea o colocada en lugares protegidos de los impactos. Los focos de iluminación de blancos y de iluminación general estarán protegidos por los parabalas o por parabalas especialmente colocados para su protección.

Criterio de evaluación

Una vez analizados todos los puntos anteriormente expresados y evaluados conjuntamente, la galería reúne las debidas condiciones de seguridad cuando:

a) Existe la certeza de que ninguna bala pueda salirse de los límites de la galería.

b) Las protecciones son las adecuadas al máximo calibre a usar.

c) Ninguna persona puede ser alcanzada durante las tiradas por un disparo entre los puestos de tirador y el espaldón.

B) CAMPOS DE TIRO

1. Zona de seguridad

a) La zona de seguridad es la comprendida dentro de un sector circular de 45 grados a ambos lados del tirador y 200 metros de radio, distribuido en las siguientes zonas:

1. Hasta 60 metros, zona de efectividad del disparo.
2. Hasta 100 metros, zona de caída de platos o pichones.
3. Hasta 200 metros, zona de caída de plomos sin ninguna efectividad pero sí molestos. Esta zona puede disminuirse según las características del terreno, por ejemplo, si está en pendiente ascendente, o tiene espaldón natural.

b) La zona de seguridad debe estar desprovista de todo tipo de edificaciones y carreteras por donde puedan transitar personas, animales o vehículos y que no pueda ser cortado al tránsito durante las tiradas.

c) En caso de practicarse las modalidades de tiro «Skeep» o recorrido de caza, la zona de seguridad se calculará a partir de los diversos puestos de tirador y los posibles ángulos de tiro.

d) En caso de no ser los terrenos de la zona de seguridad propiedad de la Sociedad de Tiro al Plato deberá obtenerse el consentimiento escrito de los propietarios de las fincas incluidas en dicha zona, autorizando la caída de pichones, platos y plomos durante las tiradas.

e) La zona de seguridad no debe estar cruzada por líneas aéreas, eléctricas o telefónicas, sobre las que puedan incidir los pichones, platos o plomos.

2. Protección de las máquinas lanzadoras

Las máquinas lanzadoras así como sus sirvientes deben estar protegidos dentro de una construcción subterránea de techo de hormigón, ya que sus sirvientes estarán siempre dentro de la línea de tiro.

La cota del nivel superior del forjado del techo debe corresponder a la. 0,00 respecto de la de los puestos de tiro.

3. Protección de los espectadores

La zona reservada a los espectadores deberá estar a la espalda de los tiradores y los accesos al campo serán por la parte trasera o como máximo perpendicular a la línea de tiro. En caso de duda, se colocarán unas pantallas laterales al tirador que limiten el ángulo de tiro.

4. Cierre o señalización

Lo ideal es que el campo con su zona de seguridad esté vallado en todo su perímetro. Este supuesto no ocurre con mucha frecuencia ya que en la mayoría de los casos están instalados en terrenos comunales que no se pueden cerrar, en cuyo caso se exigirá:

a) Que durante las tiradas se cierre la zona de seguridad mediante vallas enrollables de alambre.
b) Que a lo largo del perímetro de seguridad y cada 50 metros, como mínimo, se coloquen carteles indicativos bien visibles de la existencia del campo y banderolas rojas cuando hay tiro.
c) Que durante las tiradas, se cierren todos los caminos o pistas forestales que atraviesen la zona de seguridad, no permitiendo el paso de persona ni por supuesto su permanencia dentro de la zona de seguridad.
d) Por ser en este último supuesto las señalizaciones de carácter no perdurable, se hará constar expresamente en las autorizaciones que las tiradas y los entrenamientos estarán condicionados a la comprobación por la Guardia Civil de la existencia de aquéllas, así como que se han cerrado al tráfico todos los caminos, carreteras y accesos que atraviesen la zona de seguridad.

Criterio de evaluación

Un campo de tiro reúne condiciones de seguridad cuando, examinados cada uno de los puntos anteriores y todos en conjunto:

a) Ninguna persona que ha cumplido con las señalizaciones de seguridad impuestas durante la tirada puede ser alcanzada entre los puestos de tirador y el límite del campo.
b) Las señalizaciones son claras, bien visibles y no ofrecen ninguna duda.

INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 2

Normas y técnicas de inutilización de las armas de fuego para garantizar que las armas de fuego inutilizadas lo sean irreversiblemente

1. Objeto y ámbito de aplicación

De conformidad con el artículo 108 de este Reglamento, esta ITC tiene por objeto establecer las normas y técnicas de inutilización de las armas de fuego reglamentarias, a fin de garantizar que las modificaciones realizadas conviertan a todos sus componentes esenciales en permanentemente inservibles e impidan que puedan retirarse, sustituirse o modificarse de manera que el arma de fuego pueda reutilizarse de algún modo.

Esta ITC no será aplicable a las armas de fuego inutilizadas con anterioridad a su fecha de entrada en vigor, a menos que dichas armas de fuego sean transferidas a otro Estado miembro de la Unión Europea o comercializadas, incluida la transferencia gratuita, la herencia, el intercambio o el trueque.

Se asimilan al régimen de tenencia de las armas de fuego inutilizadas aquellas que han sido seccionadas longitudinalmente en todas sus piezas fundamentales dejando ver los mecanismos interiores y que se utilizan con el único propósito de enseñanza en los centros autorizados para ello.

2. Personas y entidades autorizadas a inutilizar armas de fuego

1. La inutilización de un arma de fuego sólo podrá ser realizada por un banco oficial de pruebas o por un armero autorizado por la Dirección General de la Guardia Civil. La inutilización de las armas de guerra o las de dotación de las Fuerzas Armadas, la Policía Nacional y el Cuerpo de la Guardia Civil, se llevará a cabo por los Centros autorizados por el Ministerio de Defensa o los Servicios de Armamento de la Policía Nacional o de la Guardia Civil.

3. Verificación de la inutilización de las armas de fuego

Un banco oficial de pruebas autorizado por la Dirección General de la Guardia Civil u otra entidad verificadora designada por el Ministerio de Defensa, la Dirección de la Policía Nacional o la Dirección General de la Guardia Civil, en el caso de armas de guerra o de dotación de dichas Fuerzas o Cuerpos, verificará que la inutilización de las armas de fuego se ha llevado a cabo con arreglo a las especificaciones técnicas de esta ITC.

Si la entidad verificadora también está autorizada a inutilizar armas de fuego, la Dirección General de la Guardia Civil garantizará que dichas tareas y las personas que las llevan a cabo estén claramente separadas dentro de la entidad.

Las entidades verificadoras autorizadas comunicarán a la Dirección General de la Guardia Civil sus datos identificativos, su símbolo y los datos de contacto, al objeto de su integración en la página web de la Comisión europea.

4. Certificado de inutilización

Si la inutilización de un arma de fuego ha sido llevada a cabo de conformidad con las especificaciones técnicas establecidas en el anexo I, la entidad verificadora o banco oficial de pruebas autorizado deberá extender al propietario del arma un certificado de inutilización conforme al modelo que figura en el anexo III. Toda la información que conste en el certificado de inutilización deberá proporcionarse en castellano y en inglés.

El propietario de un arma de fuego inutilizada conservará el certificado de inutilización en todo momento. Si se comercializa el arma de fuego inutilizada, deberá ir acompañada del certificado de inutilización.

La Dirección General de la Guardia Civil y las entidades verificadoras llevarán un registro de los certificados de armas de fuego inutilizadas que se extiendan, en el que constará, al menos, la fecha de inutilización, número de certificado, el número de la autorización y número de documento de identidad del titular del arma y reseña de las armas de fuego que se inutilicen. Dicha información se conservará durante los plazos establecidos en el artículo 9 de este Reglamento.

5. Marcado de las armas de fuego inutilizadas

Las armas de fuego inutilizadas irán marcadas con un marcado único común de conformidad con el modelo establecido en el anexo II para indicar que han sido inutilizadas con arreglo a las especificaciones técnicas establecidas en el anexo I. La entidad verificadora fijará el marcado en todos los componentes esenciales modificados por la inutilización del arma de fuego de acuerdo con los siguientes criterios:

a) Será claramente visible e inamovible.

b) Llevará la información del país en que se ha llevado a cabo la inutilización y de la entidad verificadora que la ha certificado.

c) Conservará el número o números de serie originales del arma de fuego.

Los Estados miembros reconocerán los certificados de inutilización extendidos por otro Estado miembro si dichos certificados cumplen los requisitos establecidos en esta ITC.

6. Medidas de inutilización adicionales

La Dirección General de la Guardia Civil podrá introducir medidas adicionales para inutilizar armas de fuego que vayan más allá de las especificaciones técnicas establecidas en el anexo I, previa notificación a la Comisión europea.

La Dirección General de la Guardia Civil podrá exigir la prueba de que las armas de fuego inutilizadas que se vayan a transferir a su territorio cumplen dichas medidas adicionales.

ANEXO I

Especificaciones técnicas para la inutilización de armas de fuego

1. Las operaciones de inutilización que deben realizarse para que las armas de fuego inutilizadas lo sean irreversiblemente se definen mediante tres cuadros:

a) En el cuadro I figuran los distintos tipos de armas de fuego.

b) En el cuadro II se establecen los principios generales que deben seguirse al inutilizar irreversiblemente las armas de fuego.

c) En el cuadro III se describen las operaciones específicas por tipo de arma de fuego que deben realizarse para inutilizar irreversiblemente las armas de fuego.

2. Las especificaciones técnicas para la inutilización de las armas de fuego deben impedir la reactivación de las armas de fuego utilizando herramientas corrientes.

3. Las especificaciones técnicas para la inutilización de las armas de fuego se centran en la inutilización de los componentes esenciales de las armas de fuego, definidos en este Reglamento. Las especificaciones técnicas para la inutilización de armas de fuego establecidas en el anexo I se aplican también a la inutilización de los cañones de recambio que, como objetos separados, estén técnicamente vinculados y destinados a ser montados en el arma de fuego que se inutiliza.

Cuadro I. Lista de tipos de armas de fuego

1	Pistolas (de disparo único, semiautomáticas).
2	Revólveres (incluidos los revólveres con tambor de repuesto).
3	Armas de fuego largas de un solo tiro (sin acción basculante).
4	Armas de fuego de acción basculante (por ejemplo, armas de fuego cortas y largas con cañón de ánima lisa, rayada o una combinación de ambas, de cierre levadizo o pivotante).
5	Armas de fuego largas de repetición (cañón de ánima lisa o rayada).
6	Armas de fuego largas semiautomáticas (cañón de ánima lisa o rayada).
7	Armas de fuego (completamente) automáticas, por ejemplo: determinados fusiles de asalto, metralletas y ametralladoras, pistolas (completamente) automáticas.
8	Armas de fuego de avancarga.

Cuadro II. Principios generales

1. Impedir el desmontaje de los componentes esenciales de las armas de fuego mediante soldadura o unión, o utilizando medidas adecuadas con un grado de permanencia equivalente.
2. Este proceso puede llevarse a cabo tras una comprobación por la entidad verificadora.
3. Dureza de las piezas insertadas: los bancos oficiales de pruebas o armeros autorizados para realizar la inutilización de un arma de fuego garantizarán que los pasadores, tapones y varas utilizados tienen una dureza mínima de 40 HRC y que el material de soldadura utilizado asegura una unión permanente y eficaz.

Cuadro III. Operaciones específicas por tipo de arma

1. Pistolas (de disparo único, semiautomáticas)	
1.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la recámara si existe (anchura: superior a la mitad del calibre; longitud: en caso de ánima rayada, tres veces la longitud de la recámara; en caso de ánima lisa, dos veces la longitud de la recámara).

1. Pistolas (de disparo único, semiautomáticas)	
1.2	Cañón: en todas las pistolas, salvo las de cañón con acción basculante, practicar un orificio que atraviese ambas paredes de la recámara e insertar en él un pasador de acero templado (de diámetro superior a la mitad del de la recámara, con un mínimo de 4,5 mm), que se inmovilizará por soldadura. El mismo pasador podrá utilizarse para asegurar el cañón a la acción. Alternativamente, insertar en la recámara un tapón del tamaño de la vaina del cartucho e inmovilizarlo por soldadura.
1.3	Cañón: quitar la rampa de alimentación, en su caso.
1.4	Cañón: asegurar el cañón permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia. El pasador utilizado en la operación 1.2 puede utilizarse con este fin.
1.5	Cañón: en el caso de cañones de recambio que no formen parte de una pistola, practicar las operaciones 1.1 a 1.4 y 1.19 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
1.6	Cerrojo o cabeza de cierre: quitar o acortar el percutor.
1.7	Cerrojo o cabeza de cierre: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la cara del cierre. Todos los tetones de acerrojado deberán eliminarse o rebajarse considerablemente.
1.8	Cerrojo o cabeza de cierre: soldar el orificio del percutor.
1.9	Cierre en corredera: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la superficie.
1.10	Cierre en corredera: quitar el percutor.
1.11	Cierre en corredera: eliminar los tetones de acerrojado de la corredera.
1.12	Cierre en corredera: en su caso, fresar la parte interior del borde de acerrojado del mecanismo eyector en la corredera con un ángulo de entre 45 y 75 grados.
1.13	Cierre en corredera: si la cabeza de cierre puede quitarse del cuerpo de la corredera, será preciso fijar permanentemente la cabeza de cierre inutilizada al cuerpo de la corredera.
1.14	Armazón/cajón de los mecanismos: quitar la rampa de alimentación, en su caso.
1.15	Armazón/cajón de los mecanismos: eliminar por fresado dos tercios, como mínimo, de las guías de la corredera en los dos lados del armazón.
1.16	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
1.17	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
1.18	Sistema automático: destruir el pistón de gas, el tubo de gas y el sistema de gas por corte o soldadura.
1.19	Sistema automático: si no hay pistón de gas, quitar el tubo de gas. Si el cañón se utiliza como pistón de gas, soldar el cañón inutilizado a la caja. En todos los casos en que exista, cerrar la válvula de gas del cañón mediante soldadura.
1.20	Cargadores: unir el cargador con puntos de soldadura o utilizar medidas adecuadas con un grado equivalente de permanencia, dependiendo del tipo de arma y material, para impedir la retirada del cargador.
1.21	Cargadores: si falta el cargador, poner puntos de soldadura o utilizar medidas adecuadas en la ubicación del cargador o fijar un tope para impedir de forma permanente que se introduzca un cargador.
1.22	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.
1.23	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

2. Revólveres (incluidos los revólveres con tambor de repuesto)	
2.1	Cañón: abrir una ranura longitudinal (anchura: superior a la mitad del calibre; longitud: como mínimo, la mitad de la longitud del cañón, desde el cono de forzamiento).
2.2	Cañón: practicar un orificio que atraviese ambas paredes del cañón (cerca del cono de forzamiento), por el que se insertará un pasador de acero templado, que se inmovilizará por soldadura (diámetro superior a la mitad del calibre, con un mínimo de 4,5 mm). El mismo pasador podrá utilizarse para asegurar el cañón a la acción. Alternativamente, inmovilizar por soldadura un tapón de acero templado que encaje (longitud: como mínimo la mitad de la longitud de la recámara del tambor) dentro del cañón, desde el lado del tambor.
2.3	Cañón: asegurar el cañón permanentemente al armazón mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia. El pasador utilizado en la operación 2.2 puede utilizarse con este fin.

2. Revólveres (incluidos los revólveres con tambor de repuesto)	
2.4	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 2.1 a 2.3 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
2.5	Tambor: eliminar mediante fresado dos tercios, como mínimo, de la longitud total de las paredes internas del tambor. Eliminar la mayor parte posible de las paredes internas del tambor, idealmente hasta el diámetro de la vaina, sin romper la pared exterior.
2.6	Tambor: cuando sea posible, impedir mediante soldadura que se separe el tambor del armazón o adoptar medidas adecuadas, como insertar un pasador, para que la separación sea imposible.
2.7	Tambor: en el caso de tambores de repuesto que no estén fijados a un arma, practicar la operación 2.5. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los tambores puedan ser fijados a un arma.
2.8	Armazón/cajón de los mecanismos: ampliar el orificio del percutor a tres veces su tamaño original.
2.9	Armazón/cajón de los mecanismos: quitar o acortar el percutor.
2.10	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
2.11	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
2.12	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.
2.13	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

3. Armas de fuego largas de un solo tiro (sin acción basculante)	
3.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la recámara si existe (anchura: superior a la mitad del calibre; longitud: en caso de ánima rayada, tres veces la longitud de la recámara; en caso de ánima lisa, dos veces la longitud de la recámara).
3.2	Cañón: practicar un orificio que atraviese ambas paredes de la recámara e insertar en él un pasador de acero templado (de diámetro superior a la mitad del de la recámara, con un mínimo de 4,5 mm), que se inmovilizará por soldadura. El mismo pasador podrá utilizarse para asegurar el cañón a la acción. Alternativamente, insertar en la recámara un tapón del tamaño de la vaina del cartucho e inmovilizarlo por soldadura.
3.3	Cañón: quitar la rampa de alimentación, en su caso.
3.4	Cañón: asegurar el cañón permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia. El pasador utilizado en la operación 3.2 puede utilizarse con este fin.
3.5	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 3.1 a 3.4 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
3.6	Cerrojo o cabeza de cierre: quitar o acortar el percutor.
3.7	Cerrojo o cabeza de cierre: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la cara del cierre. Todos los tetones de acerrojado deberán eliminarse o rebajarse considerablemente.
3.8	Cerrojo o cabeza de cierre: soldar el orificio del percutor.
3.9	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
3.10	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
3.11	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.

3. Armas de fuego largas de un solo tiro (sin acción basculante)	
3.12	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

4. Armas de fuego de acción basculante (por ejemplo, armas de fuego cortas y largas con cañón de ánima lisa, rayada o una combinación de ambas, de cierre levadizo o pivotante)	
4.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la recámara si existe (anchura: superior a la mitad del calibre; longitud: en caso de ánima rayada, tres veces la longitud de la recámara; en caso de ánima lisa, dos veces la longitud de la recámara). En el caso de armas sin recámara en el cañón, abrir una ranura longitudinal (anchura: superior a la mitad del calibre; longitud: como mínimo, la mitad de la longitud del cañón, desde el cono de forzamiento).
4.2	Cañón: un tapón que encaje firmemente, con una longitud mínima de dos tercios la de la recámara, se inmovilizará por soldadura en la recámara y se colocará lo más cerca posible de la cabeza del cierre.
4.3	Cañón: quitar la rampa de alimentación, en su caso.
4.4	Cañón: asegurar el cañón permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia.
4.5	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 4.1 a 4.4 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
4.6	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
4.7	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
4.8	Acción: fresar un cono de 60 grados, como mínimo (ángulo del ápice), con el fin de obtener un diámetro de la base igual a 10 mm, como mínimo, o igual al diámetro de la cara del cierre.
4.9	Acción: quitar el percutor, ensanchar el orificio del percutor para que tenga un diámetro mínimo de 5 mm y soldar el orificio del percutor.
4.10	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.
4.11	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

5. Armas de fuego largas de repetición (con cañón de ánima lisa o rayada)	
5.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la recámara si existe (anchura: superior a la mitad del calibre; longitud: en caso de ánima rayada, tres veces la longitud de la recámara; en caso de ánima lisa, dos veces la longitud de la recámara). En el caso de armas sin recámara en el cañón, abrir una ranura longitudinal (anchura: superior a la mitad del calibre; longitud: como mínimo, la mitad de la longitud del cañón, desde el cono de forzamiento).
5.2	Cañón: practicar un orificio que atraviese ambas paredes de la recámara e insertar en él un pasador de acero templado (de diámetro superior a la mitad del de la recámara, con un mínimo de 4,5 mm), que se inmovilizará por soldadura. El mismo pasador podrá utilizarse para asegurar el cañón a la acción. Alternativamente, insertar en la recámara un tapón del tamaño de la vaina del cartucho e inmovilizarlo por soldadura.
5.3	Cañón: quitar la rampa de alimentación, en su caso.
5.4	Cañón: asegurar el cañón permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia. El pasador utilizado en la operación 5.2 puede utilizarse con este fin.
5.5	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 5.1 a 5.4 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
5.6	Cerrojo o cabeza de cierre: quitar o acortar el percutor.
5.7	Cerrojo o cabeza de cierre: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la cara del cierre. Todos los tetones de acerrojado deberán eliminarse o rebajarse considerablemente.
5.8	Cerrojo o cabeza de cierre: soldar el orificio del percutor.

5. Armas de fuego largas de repetición (con cañón de ánima lisa o rayada)	
5.9	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
5.10	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
5.11	Cargadores: unir el cargador con puntos de soldadura o utilizar medidas adecuadas con un grado equivalente de permanencia, dependiendo del tipo de arma y material, para impedir la retirada del cargador.
5.12	Cargadores: si falta el cargador, poner puntos de soldadura o utilizar medidas adecuadas en la ubicación del cargador o fijar un tope para impedir de forma permanente que se introduzca un cargador.
5.13	Cargadores: en el caso de cargadores de tubo, insertar uno o varios pasadores de acero templado a través del cargador, la recámara y el armazón, conectándolos permanentemente entre sí. Inmovilizar por soldadura.
5.14	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.
5.15	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

6. Armas de fuego largas semiautomáticas (con cañón de ánima lisa o rayada)	
6.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la recámara si existe (anchura: superior a la mitad del calibre; longitud: en caso de ánima rayada, tres veces la longitud de la recámara; en caso de ánima lisa, dos veces la longitud de la recámara). En el caso de armas sin recámara en el cañón, abrir una ranura longitudinal (anchura: superior a la mitad del calibre; longitud: como mínimo, la mitad de la longitud del cañón, desde el cono de forzamiento).
6.2	Cañón: practicar un orificio que atraviese ambas paredes de la recámara e insertar en él un pasador de acero templado (de diámetro superior a la mitad del de la recámara, con un mínimo de 4,5 mm), que se inmovilizará por soldadura. El mismo pasador podrá utilizarse para asegurar el cañón a la acción. Alternativamente, insertar en la recámara un tapón del tamaño de la vaina del cartucho e inmovilizarlo por soldadura.
6.3	Cañón: quitar la rampa de alimentación, en su caso.
6.4	Cañón: asegurar el cañón permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia. El pasador utilizado en la operación 6.2 puede utilizarse con este fin.
6.5	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 6.1 a 6.4 y 6.12 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
6.6	Cerrojo o cabeza de cierre: quitar o acortar el percutor.
6.7	Cerrojo o cabeza de cierre: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la cara del cierre. Todos los tetones de acerrojado deberán eliminarse o rebajarse considerablemente.
6.8	Cerrojo o cabeza de cierre: soldar el orificio del percutor.
6.9	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
6.10	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
6.11	Sistema automático: destruir el pistón de gas, el tubo de gas y el sistema de gas por corte o soldadura.
6.12	Sistema automático: si no hay pistón de gas, quitar el tubo de gas. Si el cañón se utiliza como pistón de gas, soldar el cañón inutilizado a la caja. En todos los casos en que exista, cerrar la válvula de gas del cañón mediante soldadura.
6.13	Sistema automático: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la superficie de la cara del cierre y otros lugares, de manera que la masa del cerrojo o de la cabeza de cierre quede reducida, como mínimo, en un 50 %. Asegurar la cabeza de cierre permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia.
6.14	Sistema automático: en los casos en que las cabezas de cierre estén incorporadas a un cuerpo del cerrojo, este deberá reducirse, como mínimo, en un 50 %. La cabeza de cierre deberá fijarse permanentemente al cuerpo y este deberá fijarse permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia.

6. Armas de fuego largas semiautomáticas (con cañón de ánima lisa o rayada)	
6.15	Cargadores: unir el cargador con puntos de soldadura o utilizar medidas adecuadas con un grado equivalente de permanencia, dependiendo del tipo de arma y material, para impedir la retirada del cargador.
6.16	Cargadores: si falta el cargador, poner puntos de soldadura o utilizar medidas adecuadas en la ubicación del cargador o fijar un tope para impedir de forma permanente que se introduzca un cargador.
6.17	Cargadores: en el caso de cargadores de tubo, insertar uno o varios pasadores de acero templado a través del cargador, la recámara y el armazón, conectándolos permanentemente entre sí. Inmovilizar por soldadura.
6.18	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.
6.19	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

7. Armas de fuego automáticas (por ejemplo, fusiles de asalto, metralletas y ametralladoras, pistolas automáticas)	
7.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la recámara si existe (anchura: superior a la mitad del calibre; longitud: en caso de ánima rayada, tres veces la longitud de la recámara; en caso de ánima lisa, dos veces la longitud de la recámara).
7.2	Cañón: practicar un orificio que atraviese ambas paredes de la recámara e insertar en él un pasador de acero templado (de diámetro superior a la mitad del de la recámara, con un mínimo de 4,5 mm), que se inmovilizará por soldadura. El mismo pasador podrá utilizarse para asegurar el cañón a la acción. Alternativamente, insertar en la recámara un tapón del tamaño de la vaina del cartucho e inmovilizarlo por soldadura.
7.3	Cañón: quitar la rampa de alimentación, en su caso.
7.4	Cañón: asegurar el cañón permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia. El pasador utilizado en la operación 7.2 puede utilizarse con este fin.
7.5	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 7.1 a 7.3 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
7.6	Cerrojo o cabeza de cierre: quitar o acortar el percutor.
7.7	Cerrojo o cabeza de cierre: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la cara del cierre. Todos los tetones de acerrojado deberán eliminarse o rebajarse considerablemente.
7.8	Cerrojo o cabeza de cierre: soldar el orificio del percutor.
7.9	Cierre en corredera (pistolas automáticas): fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la superficie.
7.10	Cierre en corredera (pistolas automáticas): quitar el percutor.
7.11	Cierre en corredera (pistolas automáticas): eliminar los tetones de acerrojado de la corredera.
7.12	Cierre en corredera (pistolas automáticas): en su caso, fresar la parte interior del borde de acerrojado del mecanismo eyector en la corredera con un ángulo de entre 45 y 75 grados.
7.13	Cierre en corredera (pistolas automáticas): si la cabeza de cierre puede quitarse del cuerpo de la corredera, será preciso fijar permanentemente la cabeza de cierre inutilizada al cuerpo de la corredera.
7.14	Armazón/cajón de los mecanismos (pistolas automáticas): quitar la rampa de alimentación, en su caso.
7.15	Armazón/cajón de los mecanismos (pistolas automáticas): eliminar por fresado dos tercios, como mínimo, de las guías de la corredera en los dos lados del armazón.
7.16	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
7.17	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
7.18	Sistema automático: destruir el pistón de gas, el tubo de gas y el sistema de gas por corte o soldadura.
7.19	Sistema automático: si no hay pistón de gas, quitar el tubo de gas. Si el cañón se utiliza como pistón de gas, soldar el cañón inutilizado a la caja. En todos los casos en que exista, cerrar la válvula de gas del cañón mediante soldadura.
7.20	Sistema automático: fresar o eliminar la cara del cierre con un ángulo de entre 45 y 75 grados, medido a partir del ángulo de la cara original. Deberá eliminarse material de toda la superficie de la cara del cierre y otros lugares, de manera que la masa del cerrojo o de la cabeza de cierre quede reducida, como mínimo, en un 50 %. Asegurar la cabeza de cierre permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia.

7. Armas de fuego automáticas (por ejemplo, fusiles de asalto, metralletas y ametralladoras, pistolas automáticas)	
7.21	Sistema automático: en los casos en que las cabezas de cierre estén incorporadas a un cuerpo del cerrojo, este deberá reducirse, como mínimo, en un 50 %. La cabeza de cierre deberá fijarse permanentemente al cuerpo y este deberá fijarse permanentemente al arma mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia.
7.22	Cargadores: unir el cargador con puntos de soldadura o utilizar medidas adecuadas con un grado equivalente de permanencia, dependiendo del tipo de arma y material, para impedir la retirada del cargador.
7.23	Cargadores: si falta el cargador, poner puntos de soldadura o utilizar medidas adecuadas en la ubicación del cargador o fijar un tope para impedir de forma permanente que se introduzca un cargador.
7.24	Cargadores: en el caso de cargadores de tubo, insertar uno o varios pasadores de acero templado a través del cargador, la recámara y el armazón, conectándolos permanentemente entre sí. Inmovilizar por soldadura.
7.25	Silenciador o supresor: impedir permanentemente que se separe el silenciador o supresor del cañón, con un pasador de acero templado o mediante soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, si el silenciador forma parte del arma.
7.26	Silenciador o supresor: quitar, en lo posible, todas las partes internas del silenciador y sus puntos de fijación, de forma que solo quede un tubo. Practicar orificios cuyo diámetro sea mayor que el calibre del arma, a intervalos longitudinales de 3 (armas cortas) o 5 cm (armas largas), a través del tubo y penetrando en la cámara de expansión. Alternativamente, abrir una ranura longitudinal de 6 mm como mínimo desde el extremo posterior hasta el anterior a través del tubo y penetrando en la cámara de expansión.

8. Armas de fuego de avancarga, incluidas las de acción basculante (excepto los revólveres con tambor de repuesto)	
8.1	Cañón: abrir una ranura longitudinal a través del cañón, incluida la cámara de combustión si existe (anchura: superior a la mitad del calibre; longitud: tres veces el diámetro del proyectil). En el caso de armas sin cámara de combustión en el cañón, abrir una ranura longitudinal (anchura: superior a la mitad del calibre; longitud: como mínimo, la mitad de la longitud del cañón, desde el cono de forzamiento).
8.2	Cañón: en el caso de armas con cámara de combustión en el cañón, practicar un orificio que atraviese ambas paredes de la cámara de combustión e insertar en él un pasador de acero templado (de diámetro superior a la mitad del de la cámara, con un mínimo de 4,5 mm), que se inmovilizará por soldadura. El mismo pasador podrá utilizarse para asegurar el cañón a la acción. En el caso de armas sin cámara de combustión en el cañón, inmovilizar por soldadura un tapón de acero templado que encaje dentro del cañón (longitud: como mínimo, el doble del diámetro del proyectil), desde el cono de forzamiento.
8.3	Cañón: en el caso de cañones de recambio que no estén fijados a un arma, practicar las operaciones 8.1 a 8.2 según convenga. Además, debe impedirse permanentemente, mediante cortes, soldadura, adhesión o medidas adecuadas con un grado equivalente de permanencia, que los cañones puedan ser fijados a un arma.
8.4	En caso de acción basculante: fresar un cono de 60 grados, como mínimo (ángulo del ápice), con el fin de obtener un diámetro de la base igual a 10 mm, como mínimo, o igual al diámetro de la cara del cierre.
8.5	En caso de acción basculante: quitar el percutor, ensanchar el orificio del percutor para que tenga un diámetro mínimo de 5 mm y soldar el orificio del percutor.
8.6	Mecanismo del gatillo: asegurar la destrucción del vínculo de funcionamiento físico entre el gatillo y el martillo, percutor o fiador. Fundir el mecanismo del gatillo con soldadura dentro del armazón o cajón de los mecanismos, en su caso. Si esta fusión del mecanismo del gatillo no es posible, quitar el mecanismo del gatillo y rellenar el espacio con soldadura o resina epoxi.
8.7	Mecanismo del gatillo: el mecanismo y/o la caja del gatillo deben soldarse al cajón de los mecanismos o al armazón (en caso de armazón de acero) o encolarse a estos con pegamento resistente a temperaturas elevadas (en caso de armazón de metal ligero o polímero).
8.8	Boquillas o chimeneas/orificios u oídos: quitar o soldar las boquillas o chimeneas, soldar los orificios u oídos.
8.9	Cámaras de combustión separadas o múltiples (excepto de tambor): en el caso de armas con cámaras de combustión separadas o múltiples, eliminar mediante fresado dos tercios, como mínimo, de las paredes internas de las cámaras de combustión. Eliminar la mayor parte posible de las paredes internas, idealmente hasta el diámetro del calibre.

ANEXO II

Modelo de marcado de armas de fuego inutilizadas

EU[1] aa[2] bb[3] cc[4]

[1] Marca de inutilización (dejar «EU» en todos los marcados nacionales).

[2] País de inutilización (código internacional oficial).

[3] Símbolo de la entidad que haya certificado la inutilización del arma de fuego.

[4] Año de la inutilización El marcado completo se fijará únicamente en el armazón del arma de fuego, mientras que la marca de inutilización (1) y el país de inutilización (2) irán fijados en todos los demás componentes esenciales.

ANEXO III

Modelo de certificado para armas inutilizadas

(ANNEX III)

Model certificate for deactivated firearms

(El certificado debe extenderse en papel no falsificable)

(This certificate should be prepared on non-falsifiable paper)

Logotipo de la UE	Nombre de la entidad que haya verificado y certificado la conformidad de la inutilización Logotipo (Name of entity that has verified & certified the conformity of the deactivation) (Logo)
CERTIFICADO DE INUTILIZACIÓN (DEACTIVATION CERTIFICATE) Número de certificado (Certificate number): Las medidas de inutilización cumplen los requisitos de las especificaciones técnicas para la inutilización de armas de fuego establecidas en el anexo I del Reglamento de Ejecución (UE) 2018/337 de la Comisión de 5 de marzo de 2018. (The deactivation measures conform to the requirements of the technical specifications for the deactivation of firearms as set out in Annex I to Commission Implementing Regulation (UE) 2018/337 of 5 March 2018) Nombre de la entidad que llevó a cabo la inutilización: (Name of entity that performed the deactivation) País: (Country) Fecha/año en que se certificó la inutilización: (Date/year of certification of the deactivation) Fabricante/marca del arma de fuego inutilizada: *(Manufacturer/brand of firearm deactivated)* Tipo: *(Type)* Marca/Modelo: *(Mark/model)* Calibre: *(calibre)* Número(s) de serie: *(Serial number)* Observaciones: *(Remarks)*	
Marca de inutilización oficial de la UE *(Official EU deactivation mark)*	Nombre, cargo y firma del responsable *(Name, title and signature of the responsible person)*
Nota: Este certificado es un documento importante y el propietario del arma de fuego inutilizada debe conservarlo en todo momento. Los componentes esenciales del arma de fuego inutilizada objeto de este certificado han sido señalados con una marca de inspección oficial; dicha marca no debe retirarse ni modificarse. *(Please note: This certificate is an important document. It should be retained by the owner of the deactivated firearm at all times. The essential components of the deactivated firearm to which this certificate relates have been marked with an official inspection mark; that mark must not be removed or altered)* ADVERTENCIA: La falsificación de un certificado de inutilización podría constituir una infracción penal con arreglo al Derecho nacional. *(WARNING: Forging a deactivation certificate could constitute and offence under the national law)*	

INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 3

Armas de alarma y señales

1. Generalidades

Esta Instrucción Técnica transpone la Directiva de Ejecución (UE) 2019/69 de la Comisión de 16 de enero de 2019 que establece especificaciones técnicas para las armas de alarma y de señalización con arreglo a la Directiva 91/477/CEE del Consejo, sobre el control de la adquisición y tenencia de armas.

Tiene por objeto establecer las especificaciones técnicas que deben cumplir las armas de alarma y señales para su fabricación e importación a España, con el fin de que no puedan transformarse para lanzar un perdigón, una bala o un proyectil por la acción de un

combustible propulsor. Las armas de alarma y señales que no cumplan las especificaciones técnicas establecidas en esta ITC y su Anexo, serán clasificadas como armas de fuego en su correspondiente categoría.

2. Acreditación

Para la fabricación e importación a España de armas de alarma y señales se acreditará el cumplimiento de las especificaciones técnicas recogidas en el Anexo de esta ITC, mediante un certificado del banco oficial de pruebas español u otro documento acreditativo de una entidad reconocida por un Estado miembro de la Unión Europea.

3. Intercambio de información

La Intervención Central de Armas y Explosivos solicitará o facilitará los resultados de las comprobaciones realizadas para determinar la conformidad de las armas de alarma y señales con la especificaciones técnicas del Anexo de esta ITC a las autoridades competentes de otros Estados miembros que lo soliciten.

4. Registro de armas de alarma y señales

El banco oficial de pruebas llevará, por medios electrónicos, informáticos o telemáticos, un registro de los certificados de armas de alarma y señales que extiendan, en el que constará, al menos, el número de certificado, identidad del solicitante y fabricante, procedencia, marca, modelo, calibre y numeración del arma.

Asimismo, el banco oficial de pruebas comunicará a la Intervención Central de Armas y Explosivos los fabricantes, países de procedencia, marcas, modelos y calibres de las armas de alarma y señales que cumplan las especificaciones técnicas de esta ITC para su inscripción en el Registro Nacional de Armas.

ANEXO

Especificaciones técnicas de las armas de alarma y señales

1. Los dispositivos estarán fabricados de modo que cumplan los requisitos siguientes:

a) puedan disparar cartuchos pirotécnicos de señalización únicamente si se acopla un adaptador a la boca;

b) tengan dentro un dispositivo duradero que impida disparar cartuchos cargados con uno o varios perdigones sólidos, balas sólidas o proyectiles sólidos;

c) estén diseñados para un cartucho que figura en la tabla VIII de las Tablas de las Dimensiones de Cartuchos y de Recámaras (TDCC) establecidas por la Comisión Internacional Permanente para la Prueba de Armas de Fuego Portátiles (CIP) y se ajuste a las dimensiones y normas indicadas en dicha tabla, en su versión aplicable en el momento de adoptarse la presente Directiva.

2. Los dispositivos no pueden ser modificados con herramientas corrientes para lanzar o para poder ser transformados de modo que puedan lanzar un perdigón, una bala o un proyectil por la acción de un combustible propulsor.

3. Ninguno de los componentes esenciales de los dispositivos pueda ser instalado o utilizado como componente esencial de un arma de fuego.

4. Los cañones de los dispositivos no puedan ser retirados ni modificados sin deteriorar significativamente el dispositivo o destruirlo.

5. Si el dispositivo tiene un cañón que no excede de 30 cm o una longitud total que no excede de 60 cm, llevará incorporadas barreras inamovibles en toda la longitud del cañón de modo que este no puede ser recorrido por un perdigón, una bala ni un proyectil por la acción de un combustible propulsor, y de manera que en la boca no quede ningún espacio libre de más de 1 cm de longitud.

6. Si el dispositivo no es de los contemplados en el punto 5, llevará incorporadas barreras inamovibles en por lo menos un tercio de la longitud del cañón de modo que éste no puede ser recorrido por un perdigón, una bala ni un proyectil por la acción de un combustible

propulsor, y de manera que en la boca no quede ningún espacio libre de más de 1 cm de longitud.

7. En todos los casos, ya esté el dispositivo contemplado en el punto 5 o en el punto 6, la primera barrera del cañón estará colocada lo más cerca posible después de la recámara del dispositivo, permitiendo la expulsión de gases a través de orificios de escape.

8. En el caso de los dispositivos diseñados para disparar únicamente cartuchos de fogueo, las barreras a las que se refieren el punto 5 o el punto 6 bloquearán totalmente el cañón, salvo uno o varios orificios de escape para la presión del gas. Además, las barreras bloquearán totalmente el cañón de manera que no puede dispararse gas por la parte frontal del dispositivo.

9. Todas las barreras serán permanentes e imposibles de extraer sin destruir la recámara o el cañón del dispositivo.

En los dispositivos diseñados para disparar únicamente cartuchos de fogueo, las barreras estarán hechas completamente de un material que resista el corte, el taladro, la perforación o la amoladura (o cualquier proceso similar) y que tendrá una dureza mínima de 700 HV 30 (conforme al ensayo de dureza Vickers).

En los dispositivos no contemplados en el párrafo segundo del presente punto, las barreras estarán hechas de un material que resista el corte, el taladro, la perforación o la amoladura (o cualquier proceso similar) y que tendrá dureza mínima de 610 HV 30. El cañón podrá tener un canal a lo largo de su eje que permita expulsar del dispositivo los productos irritantes u otras sustancias activas.

En cualquier caso, las barreras han de impedir:

a) practicar o ampliar un orificio en el cañón a lo largo de su eje;

b) retirar el cañón, salvo si al retirarlo se inutiliza la zona de armazón y recámara del dispositivo, o si se compromete de tal modo la integridad del dispositivo que no pueda utilizarse como base de un arma de fuego sin hacer reparaciones o añadidos importantes.

10. La recámara de cartuchos y el cañón estarán desalineados, ladeados o escalonados de manera que el dispositivo no pueda cargarse con munición ni dispararla. Además, en el caso de dispositivos de tipo revólver:

a) las aberturas frontales de la recámara cilíndrica estarán estrechadas para garantizar que las balas queden bloqueadas en la recámara;

b) esas aberturas están desalineadas respecto de la recámara.

INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 4

Especificaciones técnicas de marcado de las armas y los componentes esenciales

1. Generalidades

Esta Instrucción Técnica transpone la Directiva de Ejecución (UE) 2019/68 de la Comisión, de 16 de enero de 2019, que establece especificaciones técnicas para el marcado de las armas de fuego y sus componentes esenciales en virtud de la Directiva 91/477/CEE del Consejo, sobre el control de la adquisición y tenencia de armas.

De conformidad con el artículo 28 a 30, todas las armas de fuego y los componentes esenciales que formen parte de ellas o se comercialicen por separado, dispondrán de un marcado claro, permanente y único, aplicado a ellos sin demora tras su fabricación o importación en la Unión Europea y, en todo caso, antes de su comercialización, con arreglo a las especificaciones técnicas de esta Instrucción Técnica Complementaria.

Todas las marcas, numeraciones y señales a que hacen referencia los apartados de esta ITC, deberán efectuarse por un procedimiento que asegure su permanencia y claridad. La profundidad adecuada y el tamaño de fuente de las marcas es fundamental para evitar que se alteren o eliminen fácilmente y lograr el objetivo de incrementar la trazabilidad de las armas y sus componentes esenciales.

En todo caso la marca del armazón o cajón de mecanismos identificará el arma de fuego en los registros correspondientes, el resto de componentes esenciales que integren el arma serán registrados cuando tengan un marcado distinto al armazón o cajón de mecanismos.

Cuando un componente esencial sea demasiado pequeño para ser marcado de conformidad con este apartado, se marcará al menos con el código del país de fabricación y la numeración de fábrica.

Marcado de las armas de fuego

1. Las marcas grabadas en el arma de fuego y sus componentes esenciales tendrán un tamaño de letra mínimo de al menos 1,6 mm. Excepcionalmente, en caso de imposibilidad técnica, la Intervención Central de Armas y Explosivos podrá autorizar el empleo de un tamaño de letra inferior para el marcado de los componentes esenciales que sean demasiado pequeños.

2. En el caso de los armazones y cajones de mecanismos fabricados con un tipo de material no metálico que no garantizan la permanencia del marcado, especificado por la Intervención Central de Armas y Explosivos, el marcado se aplicará a una placa metálica permanentemente integrada en el material del armazón o del cajón de mecanismos, de tal modo que:

a) la placa no pueda eliminarse o sustituirse fácilmente y

b) eliminar la placa implicase necesariamente destrozar parte del armazón o del cajón de mecanismos.

La Intervención Central de Armas y Explosivos podrá autorizar el uso de otras técnicas de marcado que garanticen un nivel de claridad y permanencia equivalente. Asimismo, determinará qué materiales no metálicos les será de aplicación esta especificación teniendo en cuenta el grado en que estos pueden poner en peligro la claridad y permanencia del marcado.

3. El alfabeto utilizado en el marcado será el alfabeto latino.

4. El sistema de numeración utilizado en el marcado será el arábigo.

INSTRUCCIÓN TÉCNICA COMPLEMENTARIA NÚMERO 5

Tarjeta Europea de Armas de Fuego

1. Objeto

De conformidad con el artículo 113 de este Reglamento, esta ITC tiene por objeto establecer el modelo de la Tarjeta Europea de Armas de Fuego, de conformidad con la Directiva 91/477/CEE, de 18 de junio, sobre el control de la adquisición y tenencia de armas.

2. Tarjeta Europea de Armas de Fuego

La Dirección General de la Guardia Civil determinará las características físicas, numeración y medidas de seguridad de la Tarjeta Europea de Armas de Fuego, de acuerdo con el modelo que figura en el Anexo I.

La Tarjeta Europea de Armas de Fuego será plegable y los cuerpos que la forman quedarán integrados, tanto el anverso como el reverso, en un único impreso tamaño DIN-A4.

La fotografía del titular de la tarjeta será de tamaño carné, en posición de frente y descubierto.

Para relacionar los componentes esenciales que forman parte de las armas guiadas, se adjuntará el documento que figura en Anexo II.

ANEXO I

Anverso

3. Identificación de las armas de fuego / Urceni strelnych zbrani / Identifikation af skydevabnene / Kenndaten der Feuerwalfen / Tulirelvade iunnused / Προοσδιοριομος τσυ πυροβολου οπλου / Particularsof firearms / Identification des armes à feu / Identificazione delle armi da fuoco / Saujamierocuidentifikacija / Saunamuju ginklu iden tifikavimas / A lofegyverek beazonositasa / Deltalji ta'l-armi tan-nar / Identificerende kenmerken van de vuurwapens / Identylikacja broni palnej / Identificacao das armas de fogo / Identifikacia strelnych zbrani / Identifikacija strelnega orozja / Tiedot ampuma-aseesta / Identifikation av skjulvapnen.

4. Referencias de las autorizaciones relativas a las armas / Údaje uradu tykajici se zbrani / Referencer til lilladelserne vedrørende vabnene / Genehmigungen bezuglich der Waffen / Relvalubade andmed / 'Αδειες που εκδοθηκαν για το οπλο / Particulars of authorisations for firearms / Références des autorisations concernant les armes / Riferimenti delle autorizzazioni le armi / Alsauces uz saujamierocu atjaujarn / Leidimas naudotis ginkiais / A fegyvertartasi engedelyek adatai / Dettalji tal-permessi ta' l-armi tan-nar / Verwijzing naar de vergunningen betreffende de vuurwapens / Numery zezwolen dotyczacych broni / Referencias das autorizacoes relativas as armas / Poznamky o povoleniach zbrani / Navedba dovoljenji za streino orozje / Tiedot a puma-aseen hallussapitoon oikeuttavasta luvasta / Uppgifter om vapentilistanden.

5. Autorizaciones de los Estados miembros visitados / Povoteni navstivenych clenskych zemi / De besogte medlemsstaters tilladelser / Genehmigungsvermerke der besuchten Mitgliedstaaten / Külastatud liikmesrikide load / 'Αδειες που χορηγησαν τα κραπη μελη που εγιναν τοππς επισκεψης / Authorisation of Member States visited / Autorisations des États membres visités / Autorizzazioni degli Stati membri visitati / Apmekleto dalibvalstu atlaujas / Kitu vatstybiu nariu isduoti leidimai / A meglatogatott tagállamok engedelyel / Permessi mahruga mill-Istati Membri vizitati / Vergunningen van de bezochte Lidstaten / Zezwolenia odwiedzanych panstw czlonkowskich / Autorizaçoes dos Estados-Membros visitados / Povolenia navstivenych clenskych statov / Dovoljenja obiskanih drzav clanic / Vierailun kohteena olleiden jasenvalticiden antamat luvat / De besokta medlemsstaternas tillstand.

6. Datos sobre desplazamientos intracomunitarios / Informace tykajici se prevozu uvnitr Unie / Oplysninger om rejser inden for Faellesskabet / Hinweise für Reisen innerhalb der Gemeinschaft / Uhendusesiseste liikumiste andmed / Πληροφοριες γις την κυκλοφορια οπλων στην Κοινοτητα / Information on travelling within the Community / Informations relatives aux déplacements intracommunautaires / Indicazioni relative agli spostamenti intracomunitari / Informacija par parvietosanos Kopienas robezas / Informacija susijusi su kelionemis Bendrijos viduje / A közösségen beluli utazasokkal kapcsolatos tajekoztatas / Informazzjoni dwar il-moviment intrakomunitarju / Inlichtingen betreffende intracommunautaire verplaatsingen / Informacje dotyczace podrozowania na terenie UE / Informaçoes relativas as deslocaçoes intracomunitárias / Informacie tykajuce sa cestovania vnutri Spolocenstva / Podatki o potovanjih znotraj Skupnosti / Tietoja malkustamisesta unionin aluella / Upplysningar om resor inom gemenskapen.

6.1. Están prohibidos los viajes a ... con el arma / Cesta do ... se zbrani ... jezakazana / Indrejse i ... med dette vaben ... er forbudt / Eine Reise nach ... mit der Waffe ... ist verboten / Reisimine ... ... relvaga on keelatud / Απαγορευεται ταξιοι στ ... με το οπλο ... / A journey to ... with the firearm ... shall be prohibited / Un voyage en ... avec l'arme ... est interdit / Un viaggio in ... con l'arma ... è vietato / Brauciens uz ... ar ieroci ... ir aizliegts / Vyktilj ... su saunamuoju ginklu ... yra draudziama / Az alabbi orszag(ok)ba ... a kovelkezo fegyverrel ... torteno beutazas tilos / Vjagg fil- ... bi-arma ... huwa projbit / Het is verboden zich met vuurwapen ... naar ... te begeven / Podroz do ... z bronia ... jest niedozwolona / É proibida a viagem a ... com a arma ... / Cestovanie do ... so zbranou ... je zakázané / Potovanje v ... s streinim orozjem ... se prepove / Matkustaminen ... on kielletty seuraavien ampuma aseiden kanssa: ... / Inresa i ... med vapen ... ar forbjuden.

6.2. Los viajes a ... con el arma ... están sometidos a autorización / Cesta do ... se zbrani ... podleha poveleni / Indrejse i ... med detle vaben ... er betinget af godkendelse / Eine Reise nach ... mit der Waffe ... ist genehmigungspflichtig / Reisimiseks ... ... relvaga on noutav luba / Υποκειται σε αδεια ταξιοι οτ ... με το οπλο ... / A journey to ... with the firearm ... shall be subject to authorisation / Un voyage en ... avec l'arme ... est soumis à autorisation / Un viaggio in ... con l'arma ... è soggetto ad autorizzazione / Braucienz uz ... ar ieroci ... ir atlauts / Norint vykti j ... su saunamuoju ginklu ... bulina gauti oficialy leidima / Az alábbi ország(ok)ba ... a kovetkezo legyverrel ... torteno beutazás engedely hez kotott / Vjagg fil ... bl arma/armi ... huwa suggett ghall permess / Om zich met vuur wapen ... naar ... te begeven is een vergunning vereist / Podroz do ... z bronia ... wymaga zezwolenia / É sujeita a autorizaçao à viagem a ... com a arma ... / Cestovanie do ... so zbranou ... podlieha povoleniu / Za potovanje v ... s streinim orozjem ... je treba pridobiti dovoljenje / Matkustaminen ... on luvanvaraista seuraavien ampuma-asseiden kanssa: ... / Inresa i ... med vapen ... krave tillstand.

ESTADO MIEMBRO

TARJETA EUROPEA DE ARMAS DE FUEGO
EVROPSKÝ PRŮKAZ STŘELNÝCH ZBRANÍ
EUROPÆISK VÅBENPAS
EUROPÄISCHER FEUERWAFFENPASS
EUROOPA TULIRELVAPASS
ΕΥΡΩΠΑΪΚΟ ΔΕΛΤΙΟ ΠΥΡΟΒΟΛΩΝ ΟΠΛΩΝ
EUROPEAN FIREARMS PASS
CARTE EUROPÉENNE D'ARMES À FEU
CARTA EUROPEA D'ARMA DA FUOCO
EIROPAS ŠAUJAMIEROČU KARTE
EUROPOS ŠAUNAMŲJŲ GINKLŲ LEIDIMAS
EURÓPAI LÖFEGYVEROKMÁNY
KARTA EWROPEA TA' L-ARMI TAN-NAR
EUROPESE VUURWAPENPAS
EUROPEJSKA KARTA BRONI PALNEJ
CARTÃO EUROPEU DE ARMAS DE FOGO
EURÓPSKY ZBROJNÝ PAS
EVROPSKO DOVOLJENJE ZA STRELNO OROŽJE
EUROOPAN AMPUMA-ASEPASSI
EUROPEISKT SKJUTVAPENPASS
EUROPSKA ORUŽNA PROPUSNICA
ЕВРОПЕЙСКИ ПАСПОРТ ЗАОГНЕСТРЕЛНО ОРЬЖИЕ

6. Datos sobre desplazamientos intracomunitarios

— El derecho a fectuar un viaje a otro Estado miembro con una o varias armas de las categorías A, B o C mencionadas en la presente tarjeta estará supeditada a una o más autorizaciones correspondientes del Estado miembro que se visita. Dichas autorizaciones podrán anotarse en la tarjeta.

— La autorización previa antes mencionada no será en principio necesaria para efectuar un viaje con un arma de categoría C para practicar en actividades de caza o de recreación histórica o con un arma de fuego de las categoría A, B o C para la práctica del tiro deportivo siempre que se esté en posesión de la tarjeta de armas de fuego y se pueda acreditar el motivo del viaje.
No obstante, de la información facilitada con arreglo al apartado 3 del artículo 8 de la Directiva 91/477/CEE del Consejo, por los Estados miembros que prohíben o supeditan a una autorización la adquisición o tenencia en su territorio de un arma de las categorías B, C o D, se desprende que:

6.1. Los viajes a .... con el arma o armas ....

quedan prohibidos.

6.2. Los viajes a .... con el arma o armas ....

precisan autorización.

Glosario

1. Datos sobre el titular / Údaje o drziteli / Opliysninger om indehaveren / Angaben zum Passinhaber / Andmed omaniku kohta / Στοιχεια που αφορου τον κατοχο / Details of the holder / Mentions relatives au titulaire / Indicazioni relative al titolare / Ipasnieka dati / Informacija apie turėtoja / A jogosult adatai / Dettalji dwar min ghandu l-permess / Vermeldingen betreffende de houder / Informacje dotyczace posiadacza / Mençoes relativas ao titular / Údaje o drzitel'ovi / Podatki o imetniku / Passinhaltijan yksilointitiedot / Upplysningar om innehavaren.

1.1. Nombre y apellidos / Prijmeni a jmeno / Efternavn og fornavn / Name und Vorname / Perekonna-ja eesnimi / Επωνυμο και ονομα / Surname and first name / Nom et prénom / Cognome e nome / Vards un uzvards / Pavardė ir vardas / Név és keresztnév / Kunjom u isem / Naam en voornaam / Nazwisko i imie / Apelido e nome / Priezvisko a meno / Priimek in ime / Sukunimi ja etunimet / Efternamn och fornamn.

1.2. Fecha y lugar de nacimiento / Datum a misto narozeni / Fødselsdato og -sled / Geburlsdatum und -ort / Sunnikuupaev ja -koht / Ημερομηνια και τοπος γεννησης / Date and place of birth / Date et lieu de naissance / Luogo e data di nascita / Dzimsanas laiks un vieta / Gimimo data ir vieta / Szuletes helye és ideje / Data u post tat-twelid / Geboorteplaate en -datum / Data i miejsce urodzenia / Data e local de nascimento / Dátum a miesto narodenia / Datum in kraj rojstva / Syntymaaika ja paikka / Födelsedatum och plats.

1.3. Nacionalidad / Slatni prislusnost / Nationalitet / Slaatsangehorigkeit / Kodakondsus / Εθνικοτητα / Nationality / Nationalité / Nazionalità / Tautiba / Tautybė / Állampolgarsag / Nazzjonalità / Nationaliteit / Obywatelstwo / Nacionalidade / Státna prislusnosí / Drzavljanstvo / Kansalaisuus / Nationalitet.

1.4. Dirección / Adresa / Bopael / Anschrift / Aadress / Διευθυνση / Address / Adresse / Indirizzo / Adrese / Adresas / Cim / Indirizz / Adres / Adres / Ender Meço / Adresa / Naslov / Oscite / Adress.

1.5. Firma del titular / Podpis majitele / Indehaverens underskrift / Unterschrift des Passinhabers / Omaniku alikiri / Υπογραφη κατοχου / Holder's signature / Signature du titulaire / Firma del titolare / Ipasnieka paraksts / Parasas / A jogosult aláírása / Firma ta' min ghandu l-permess / Handtekening van de houder / Podpis posiadacza / Assinatura do titular / Podpis drzitel'a / Podpis imetnika / Passinhaltijan nimikirjoitus / Innehavarens namnteckning.

2. Datos de la tarjeta / Údaje o průkazu / Oplysninger om passel / Angaben zum Feuerwaffenpass / Passiandmed / Στοιχεια που αφορουν το δελτιο / Details of the pass / Mentions relatives à la carte / Indicazioni relative alla carta / Atzimes par karti / Informacija apie leidima / Az okmany adatai / Dettalji dwar il-permess / Vermeldingen betreffende de pas / Informacje dotyczacc karty / Mençoes relativas ao cartao / Údaje o pase / Podatki o dovoljenju / Passin tunnistaminen / Upplysningar om passet.

2.1. N° de tarjeta / Cislo prukazu / Passets nr. / Passnummer / Passinumber / Αριθ. σελριου / Pass No / N° de la carte / N. della carta / Kartes Nr. / Leidimo Nr. / Az okmany szama / Numru tal-karta ta' l-identità / Nummer van de pas / Numer karty / N° do cartao / C. pasu / Sl. dovoljenja / Passin número / Passets nr.

2.2. Válida hasta / Platnost do / Gyldigt indtil / Gültig bis / Kehtiv kuni / Ισχυει μεχρι / Valid until / Valable jusqu'au / Valida fino al / Deriga lidz / Galioja iki / Érvenyesseg (-ig) / Valida sa / Geldig lot / Wazna do / Válido atė / Platnost do / Veljavno do / Vim. voimassaolopaiva / Giltigt till.

2.3. Sello de la autoridad / Razitko uradu / Myndighedens stempel / Behorde/Dienstsiegel / Ametivoimu pitser / Εφραγιοα της εκοουας αρχης / Authority's stamp / Sceau de l'autorité / Timbro dell'autorità / lestades zimogs / Antspaudas / A hatosag pecsetje / Timbru ta'l-awtorità / Siempel van de bevoegde autoriteit / Pieczec urzedowa / Carimbo da autoridade / Peciatka prislusneho organu / Zig organa / Viranomaisen leima ja palvays / Myndighetens stampel.

2.4. Validez prorrogada hasta / Piatnost prodlouzena do / Gyldigheden forlaenget indtil / Gültigkeit verlangert bis / Kehtivust pikendatud kuni / Παρατεινεται μεχρι / Validity extended until / Validité prorogée au / Proroga della validità fino al / Deriguma termins pagarinats lidz / Galiojimas pratestas iki / Érvenyesseg meghosszabbitva (-ig) / Validità mgedda sa / Geldigheid verlengd tot / Waznosc przediuzona do / Validade prorrogada ate / Platnosi predizena do / Veijavnost podaljsana do / Voimassaoloa jatketlu / Gilligheten forlangs till.

2.5. Sello de la autoridad / Razitko uradu / Myndighedens stempel / Behorde/Dienstsiegel / Ametivoimu pitser / Σφραγιοα της εκοουοας αρχης / Authority's stamp / Sceau de l'autorité / Timbro dell'autorità / lestades zimogs / Anstpaudas / A hatosag pecsetje / Timbru ta'l-awtorità / Stempel van de bevoegde autoriteit / Pieczec urzedowa / Carimbo da autoridade / Peciatka prislusneho organu / Zig organa / Viranomaisen leima ja paivays / Myngighetens stampel.

Reverso

1. Datos sobre el titular

1.1. Nombre y apellidos:

1.2. Lugar y fecha de nacimiento:

1.3 Nacionalidad:

1.4 Dirección:

1.5 Firma del titular:

FOTO

2. Datos de la tarjeta

2.1. Nº de Tarjeta:

2.2 Válida hasta:

2.3 Sello de la Autoridad:
Fecha:

2.4 Validez prorrogada hasta:

2.5 Sello de la Autoridad:

Fecha:

3. Identificación de las armas de fuego

Tipo	Marca / Modelo	Calibre	Nº Fabricación	Categoría Directiva	Arma Registrada	Sello de la Autoridad

4. Referencias de las autorizaciones relativas a las armas

Arma	Autorizada el	(hasta el)	Sello de la Autoridad

5. Autorizaciones de los Estados miembro visitados

Arma	Validez de la autorización	Sello de la Autoridad y fecha

ANEXO II

Apéndice a la tarjeta europea de armas de fuego número .....

RELACIÓN de componentes esenciales asociados a la/s guía/s de pertenencia propiedad de D. ..... (DNI.....).

Arma		**Componente esencial**			
Nº	Marca	Componente	Marca	Nº	Descripción

En ..... , a ..... de ..... de 20.....

El Interventor de Armas y Explosivos

Fdo.-

§ 39

Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior

Ministerio del Interior
«BOE» núm. 114, de 13 de mayo de 2011
Última modificación: 3 de enero de 2018
Referencia: BOE-A-2011-8382

El artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal establece que la creación, modificación y supresión de los ficheros de las Administraciones Públicas sólo podrá hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente.

Al amparo de lo establecido en la citada Ley Orgánica 15/1999, de 13 de diciembre, se procedió por Orden INT/3764/2004, de 11 de noviembre, publicada en el Boletín Oficial del Estado n.º 277, de 17 de noviembre de 2004, a la adecuación de los ficheros informáticos del Ministerio del Interior que contienen datos de carácter personal, entre los que se describen y regulan los que son responsabilidad de diferentes Centros Directivos de dicho Departamento.

Con posterioridad a la entrada en vigor de la mencionada Orden INT/3764/2004, de 11 de noviembre, y debido a los numerosos cambios operados en la estructura orgánica del Ministerio, la introducción de nuevos ficheros de datos se ha llevado a cabo, en ocasiones, a través de la promulgación de nuevas Órdenes autónomas de creación de ficheros. Ello supone que, en la actualidad, nos encontremos con multiplicidad de normas que versan sobre la misma materia.

Por otro lado, con motivo de la entrada en vigor del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, resulta conveniente completar el contenido exigido por el artículo 54 de dicho Reglamento respecto de las diferentes Órdenes de creación y modificación de ficheros del Ministerio del Interior.

Asimismo, nuevas necesidades surgidas en el ámbito de diferentes Centros Directivos del Ministerio requieren de un tratamiento de datos de carácter personal, lo que implica la creación de los correspondientes ficheros.

Por tanto, con el fin de proceder a la unificación de la normativa reguladora de la totalidad de los ficheros informáticos del Ministerio del Interior en aras a los principios de claridad y simplicidad, así como de adaptar el contenido de los mismos, tanto a la estructura actual del Departamento como a lo previsto en el Real Decreto 1720/2007, de 21 de diciembre, resulta necesario llevar a cabo la promulgación de la correspondiente Orden tendente a crear, modificar y suprimir los correspondientes ficheros de dicho Departamento.

La presente Orden ha sido informada por la Agencia Española de Protección de Datos en cumplimiento de lo dispuesto en el párrafo h) del artículo 37, de la Ley Orgánica 15/1999, de 13 de diciembre.

Por consiguiente, a fin de dar cumplimiento a lo establecido en el artículo 20 de la citada Ley Orgánica 15/1999, de 13 de diciembre, así como en los artículos 52 y 54 de su Reglamento de desarrollo, por cuanto establecen sobre la creación, modificación y supresión de ficheros automatizados que contengan datos de carácter personal, dispongo:

Artículo 1. *Creación de ficheros y régimen jurídico.*

Se crean los ficheros que se relacionan y describen en el Anexo I de la presente Orden.

Tales ficheros estarán sometidos al ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, así como a su Reglamento de desarrollo.

Artículo 2. *Regulación de ficheros y régimen jurídico.*

Se incorporan y, en su caso, se modifican los ficheros relacionados y con el contenido que se describe en el Anexo II de la presente Orden:

Tales ficheros estarán sometidos al ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, así como a su Reglamento de desarrollo.

Artículo 3. *Supresión de ficheros.*

Se suprime el fichero «COMUNICACIONES DE VACACIONES» regulado en la Orden INT/1751/2002, de 20 de junio, por la que se regulan los ficheros informáticos de la Dirección General de la Policía que contienen datos de carácter personal, adecuándolos a las previsiones establecidas en la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal, y demás normativa sobre la materia, así como los ficheros regulados en la Orden INT/3764/2004, de 11 de noviembre, por la que se adecuan los ficheros informáticos del Ministerio del Interior que contienen datos de carácter personal a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y se crean nuevos ficheros cuya gestión corresponde a dicho Ministerio, indicados y con el destino que se describe en el Anexo III de la presente Orden.

Disposición adicional primera. *Responsabilidad de los ficheros.*

Los diferentes Centros Directivos del Ministerio del Interior, como Órganos responsables de sus ficheros, adoptarán las medidas necesarias para garantizar que los datos de carácter personal existentes en los mismos se usen para las finalidades y funciones de derecho público que tiene encomendadas, en relación con la Ley Orgánica 15/1999, de 13 de diciembre.

Disposición adicional segunda. *Inscripción en el Registro General de Protección de Datos.*

Los diferentes Centros Directivos del Ministerio del Interior, como Órganos responsables de sus ficheros, darán traslado de la presente Orden a la Agencia Española de Protección de Datos, en el plazo de treinta días desde su publicación en el Boletín Oficial del Estado, para que se proceda a la inscripción de sus respectivos ficheros en el Registro General de Protección de Datos, conforme a lo dispuesto en el párrafo a) del apartado segundo del artículo 39 de la Ley Orgánica 15/1999, de 13 de diciembre, así como en los artículos 55 y 58 de su Reglamento de desarrollo.

Disposición transitoria única. *Vigencia del fichero «ACCIDENTES DE TRÁFICO» de la Dirección General de Tráfico.*

El fichero «ACCIDENTES DE TRÁFICO» de la Dirección General de Tráfico permanecerá vigente hasta que se cree el fichero «REGISTRO ESTATAL DE VÍCTIMAS Y ACCIDENTES DE TRÁFICO».

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Orden y, en particular, las siguientes:

– Orden INT/1751/2002, de 20 de junio, por la que se regulan los ficheros informáticos de la Dirección General de la Policía que contienen datos de carácter personal, adecuándolos a las previsiones establecidas en la Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal, y demás normativa sobre la materia.

– Orden INT/2662/2004, de 29 de julio, por la que se regulan los ficheros de datos de carácter personal relativos a afectados por atentados terroristas cuya gestión corresponde al Ministerio del Interior.

– Orden INT/3764/2004, de 11 de noviembre, por la que se adecuan los ficheros informáticos del Ministerio del Interior que contienen datos de carácter personal a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y se crean nuevos ficheros cuya gestión corresponde a dicho Ministerio.

– Orden INT/1911/2007, de 26 de junio, por la que se crea el fichero de datos de carácter personal «Violencia doméstica y de género», en el Ministerio del Interior.

– Orden INT/2127/2007, de 28 de junio, por la que se crea el fichero automatizado de datos personales BINCIPOL, y se constituyen los ficheros de datos personales, no automatizados, integrados por los archivos físicos de documentos de los diferentes órganos y unidades de la Dirección General de la Policía y de la Guardia Civil, en el ámbito del Cuerpo Nacional de Policía.

– Orden INT/803/2008, de 13 de marzo, por la que se crean ficheros automatizados de datos de carácter personal en la Comisaría General de Seguridad Ciudadana de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía.

– Orden INT/2692/2008, de 17 de septiembre, por el que se crea el fichero automatizado de datos de carácter personal DGED-UCO, en la Comisaría General de Seguridad Ciudadana de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía.

– Orden INT/2844/2008, de 26 de septiembre, por la que se crea el fichero automatizado de datos Sistema Informático Social Penitenciario, en el Ministerio del Interior.

Disposición final única. *Entrada en vigor.*

La presente Orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

ANEXO I

Secretaría de Estado de Seguridad

1. FICHERO: REGISTRO ELECTRÓNICO DE LA GUARDIA CIVIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro Electrónico de la Guardia Civil.

a.2) Finalidad: Anotaciones registrales de los asientos electrónicos efectuado en el Registro para, en su caso, poder consultar la información registral de sus asientos.

a.3) Usos previstos: Recepción y remisión de las solicitudes, los escritos y las comunicaciones y de su documentación complementaria a la persona, órgano o unidad destinataria de la misma, así como para fines estadísticos y para responder a las consultas de los propios usuarios sobre el hecho registral.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas o representantes de personas jurídicas que, a través de la sede electrónica, accedan al Registro electrónico de la Guardia Civil, creado en virtud de la Orden INT/2936/2009, de 27 de octubre.

b.2) Procedencia y procedimiento de recogida: Por archivo de los datos introducidos en el momento de realizar el asiento.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre, apellidos, DNI/NIF, pasaporte o documento identificativo, dirección postal y electrónica, teléfono.

Datos relativos a la solicitud, escrito o comunicación presentados: fecha, hora y número de asiento registral, así como la documentación anexa que aporte la persona física o jurídica que lo presente.

No se incluirán datos especialmente protegidos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la persona, órgano o unidad destinataria de la misma.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Guardia Civil - Secretaría de Despacho, calle Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: OSUNT.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: OSUNT.

a.2) Finalidad: Seguimiento de documentación relevante disponible en INTERNET sobre el delito, el crimen organizado y otros fenómenos que afectan a la seguridad pública nacional y trasnacional.

a.3) Usos previstos: Fuente abierta de consulta para la elaboración de informes de inteligencia prospectiva sobre situación del crimen organizado en el mundo, situación de la lucha contra el crimen organizado en el mundo, tendencias y prospectiva sobre dichas materias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Búsqueda y captación de información procedente de fuentes abiertas, especialmente a través de Internet, sobre nuevas tecnologías, actividades criminales, técnicas y documentación en general sobre crimen organizado, con fines estratégicos.

b.2) Procedencia y procedimiento de recogida: Internet y, eventualmente, cualquier otra fuente pública de información (singularmente los medios de comunicación).

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Base de datos documental. Se establecerá un sistema de búsqueda basado en la fecha de elaboración del documento, fecha de subida a la red, fecha de obtención del documento, origen del documento, palabras clave y cualquier otro criterio que permita la localización del mismo. En caso de otras fuentes, el sistema de búsqueda de documentos será similar.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad; a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A Organismos internacionales y países extranjeros en aplicación de tratados o convenios en los que España sea parte.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad. Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22 - 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22 - 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: ACTUACIONES INCIDENTALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Actuaciones incidentales.

a.2) Finalidad: Recogida, estudio, tratamiento, análisis, investigación, control, fiscalización, auditoría e inspección de aquellas actuaciones que se lleven a cabo por los efectivos de los Cuerpos y Fuerzas de Seguridad del Estado en el ejercicio de sus funciones o con ocasión de ellas. Así como de aquellas otras personas que demanden cuestiones y/o extremos sobre el ejercicio o comportamiento de los indicados funcionarios o bien sean demandantes o receptoras de los servicios que aquéllos prestan:

– Recogida, estudio, tratamiento, análisis, investigación, control, fiscalización, auditoría e inspección de aquellas actuaciones relativas a fallecimientos de cualquier persona y/o funcionarios policiales en dependencias de la Dirección General de la Policía y la Guardia Civil o en cualquier otro lugar si se produce por causas no naturales.

– Recogida, estudio, tratamiento, análisis, investigación, control, fiscalización, auditoría e Inspección de aquellas actuaciones respecto a la aplicación de las garantías que acompañan a las personas privadas de libertad. Así como de aquellas situaciones en las que puedan darse posibles extralimitaciones o vulneración de los derechos de las personas que se encuentren bajo su custodia.

– Recogida, estudio, tratamiento, análisis, investigación, control, fiscalización, auditoría e Inspección respecto a las imputaciones o requerimientos judiciales que se realicen a los miembros de los Cuerpos y Fuerzas de Seguridad del Estado.

a.3) Usos previstos: Control, tratamiento, archivo, gestión y explotación de los documentos y/o datos e investigaciones relativos a los fines contemplados en el apartado anterior.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios de los Cuerpos y Fuerzas de Seguridad del Estado y personas particulares interesados en los servicios que estos prestan y/o que resulten afectadas por la vulneración de sus derechos, sean víctimas y/o formulen algún tipo de reconvención o demanda sobre el tratamiento policial llevado a efecto.

b.2) Procedencia y procedimiento de recogida: Recopilación de información a través de investigaciones, entrevistas, documentos, archivos de los Cuerpos y Fuerzas de Seguridad del Estado. Remisión por parte de particulares de documentos, denuncias, sugerencias, etc.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre, apellidos, DNI, carné profesional, categoría, firma y rúbrica, tanto de los particulares, como de los funcionarios de los Cuerpos y Fuerzas de Seguridad del Estado, Atestados, diligencias policiales y judiciales, informaciones reservadas, procedimientos disciplinarios, información sobre personas, tanto de funcionarios de los referidos Cuerpos como de personas particulares implicadas y/o reclamantes de sus derechos.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Autoridades Judiciales y Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre, y otros órganos de la Administración en virtud de lo previsto en los artículos 2 y 5.1 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad. Inspección de Personal y Servicios de Seguridad. C/ Cea Bermúdez, n.° 35-37, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: SESCOPI.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SESCOPI

a.2) Finalidad: Disponer de un instrumento ágil para la gestión de los funcionarios integrados en las Consejerías de Interior de las Misiones Diplomáticas de España y en las misiones internacionales para la resolución de conflictos.

a.3) Usos previstos: Control interno de los funcionarios integrados en las Consejerías de Interior de las Misiones Diplomáticas de España y en las misiones internacionales para la resolución de conflictos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios integrados en las Consejerías de Interior de las Misiones Diplomáticas de España y en las misiones internacionales para la resolución de conflictos.

b.2) Procedencia y procedimiento de recogida: Se llevará a cabo a través de una ficha personal, debidamente cumplimentada por el funcionario público que acceda a un puesto de trabajo en las Consejerías de Interior y en misiones internacionales para la resolución de conflictos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre y apellidos, Documento Nacional de Identidad, número de carné profesional, fecha de nacimiento, fecha de alta en la misión, cargo y teléfonos de contacto. Igualmente se recogerán datos relacionados con las vacaciones, permisos, períodos de baja por enfermedad o cualquier otra vicisitud profesional que pueda producirse durante la permanencia del funcionario en la Consejerías de Interior o en las misiones internacionales para la resolución de conflictos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Fuerzas y Cuerpos de Seguridad del Estado, en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A Organismos internacionales afectados por las Misiones Internacionales en que participen los funcionarios y países extranjeros en los que las Consejerías de Interior lleven a cabo sus funciones, en aplicación de tratados o convenios internacionales en los que España sea parte.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Cooperación Policial Internacional de la Dirección General de Relaciones Internacionales y Extranjería, C/ Amador de los Ríos, 2, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

5. FICHERO: COORDINACIÓN DE OPERACIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Coordinación de Operaciones.

a.2) Finalidad: Gestión, seguimiento y control de operaciones de crimen organizado, coordinadas o en fase de coordinación, así como el resultado de las mismas.

a.3) Usos previstos: Coordinación entre las distintas Fuerzas y Cuerpos de Seguridad del Estado y otros Servicios o Instituciones, en función de sus competencias en investigaciones sobre tráfico de drogas y otras formas de crimen organizado, así como la coordinación con otros Centros internacionales con las mismas competencias; y la gestión estadística de las citadas operaciones.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los datos son los correspondientes a las personas, bienes muebles e inmuebles y otros conceptos investigados.

b.2) Procedencia y procedimiento de recogida: Los datos son facilitados por las Fuerzas y Cuerpos de Seguridad del Estado y otros Servicios o Instituciones y relativos a sus respectivas investigaciones sobre grupos criminales dedicados al tráfico de drogas y al crimen organizado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: El Sistema de Registro de Investigaciones (SRI) gestiona y detecta las coincidencias de datos objetivos de todas las investigaciones policiales, y como complemento a esa base de datos informatizada se hace necesaria la de Coordinación de Operaciones, para la gestión integral de las coincidencias encontradas. Los datos incluidos son:

1. Investigación (nombre de la operación, número de referencia de origen y número de referencia en el SRI).
2. Personas físicas (nombre y apellidos, DNI/ NIE/ Pasaporte).
3. Personas jurídicas (denominación y NIF).
4. Teléfonos.
5. Bienes inmuebles (ubicación: localidad, calle, número).
6. Medios de transporte (vehículos, barcos, aeronaves; matrícula, nombre del medio de transporte).
7. Cuentas bancarias utilizadas (número de cuenta).
8. Páginas Web usadas para delinquir (denominación de la página en Internet).
9. Direcciones de correo electrónico (dirección completa en Internet).
10. Unidad investigadora y responsable policial (Cuerpo, Unidad y Grupo que desarrolla la investigación. Nombre y apellidos, Cuerpo, empleo, cargo, teléfonos de contacto y dirección de correo electrónico del responsable operativo de la investigación).

11. Sustancias intervenidas o investigadas (tipo de droga y cantidad aprehendida).
12. Ubicación geográfica (lugares o localidades donde se intervino).
13. Tipos y subtipos de delitos investigados (genérico y específico de cada delito conforme al Código Penal).
14. Indicadores de crimen organizado (número de detenidos).
15. Denominación de la organización criminal (nombre de la operación).
16. Efectos intervenidos o investigados (cantidad de bienes inmuebles, número y descripción de medios informáticos o audiovisuales, cantidad y denominación de productos químicos, etc).
17. Otros efectos (otros bienes intervenidos).
18. Relaciones entre personas investigadas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A Organismos internacionales y países extranjeros en aplicación de tratados o convenios en los que España sea parte.

f) Órgano responsable del fichero: Secretaria de Estado de Seguridad, c/ Amador de los Ríos, 2, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Centro de Inteligencia contra el Crimen Organizado, (CICO) calle Recoletos, 22 - 28001 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

6. FICHERO: BASE DE DATOS DE INFORMES DE SITUACIÓN DEL CRIMEN ORGANIZADO (BDIS).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Base de datos de informes de situación del crimen organizado (BDIS).

a.2) Finalidad: Tener un conocimiento más profundo de los factores que inciden en la criminalidad organizada en España, derivado de la actividad delictiva, así como estructurar, de acuerdo con criterios rigurosos y técnicos, la obtención, explotación y análisis de los datos.

a.3) Usos previstos: Elaboración del Informe de Situación del Crimen Organizado en España; aportación española al Informe de Evaluación de la Amenaza en Europa y elaboración de Informes de Inteligencia Estratégica y estadísticos sobre la lucha contra los grupos de crimen organizado.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Se recogen datos relacionados con las actividades desarrolladas por los grupos de crimen organizado que están siendo o han sido investigados.

b.2) Procedencia y procedimiento de recogida: Los datos procederán de las investigaciones policiales llevadas a cabo por las Fuerzas y Cuerpos de Seguridad del Estado, y otros Servicios o Instituciones, en función de sus competencias en materia de actividades delictivas relacionadas con el crimen organizado, así como por los Cuerpos de Policía de las Comunidades Autónomas con competencias en materia de seguridad ciudadana.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Sobre la base del desglose de las diferentes investigaciones sobre los grupos de crimen organizado que operan en España, y de conformidad con la tipificación legal de las mismas, se recogerán los siguientes datos:

Relativos a las personas investigadas: Fecha, lugar y país de nacimiento; nacionalidad, sexo; número de personas investigadas y de personas detenidas.

Datos genéricos sobre las investigaciones: identificación de la investigación; Cuerpo, Unidad y Grupo que desarrolla la investigación; fecha de inicio y cierre de la investigación; modus operandi; rutas internacionales detectadas; descripción de la estructura jerárquica utilizada por el grupo criminal, ámbito de actuación y patrimonio incautado.

Datos relativos a otras investigaciones: vinculación con otra u otras investigaciones, indicándose los números de referencia y nombres de las operaciones, Unidades policiales actuantes y otros identificadores.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar trasferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaria de Estado de Seguridad, c/ Amador de los Ríos 2, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Centro de Inteligencia contra el Crimen Organizado, (CICO) calle Recoletos, 22 - 28001 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

7. FICHERO: BASE DE DATOS DE TRATA DE SERES HUMANOS (BDTRATA).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Base de datos de trata de seres humanos (BDTRATA).

a.2) Finalidad: Tener un conocimiento más profundo del fenómeno de la trata de seres humanos y de los fenómenos delictivos asociados a ella, derivado de la actividad delictiva e infractora, así como estructurar, de acuerdo con criterios rigurosos y técnicos, la obtención, explotación y análisis de los datos.

a.3) Usos previstos: Elaboración de informes de Inteligencia Estratégica y estadísticos sobre la lucha contra la trata de seres humanos y los fenómenos delictivos asociados a ella.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Se recogerán datos relacionados con las víctimas, autores, encubridores y cómplices de infracciones penales, y de las personas identificadas en los lugares de ejercicio de la prostitución y de explotación laboral como encargados, propietarios, o empleados, y de personas identificadas en las inspecciones administrativas llevadas a cabo.

b.2) Procedencia y procedimiento de recogida: Los datos procederán de las diligencias policiales y de las inspecciones administrativas, llevadas a cabo por las Fuerzas y Cuerpos de Seguridad del Estado, así como por los Cuerpos de Policía de las Comunidades Autónomas con competencias en materia de seguridad ciudadana.

Respecto a las inspecciones administrativas, únicamente se recogerán aquellos datos que sean necesarios para la investigación criminal.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos relativos a la comisión de infracciones penales y administrativas relacionadas con la trata de seres humanos y de los fenómenos delictivos asociados a ella, de conformidad con la tipificación legal de las mismas.

Datos de carácter identificativo: DNI/NIE/pasaporte/, o equivalente.
Datos de características personales: fecha, lugar y país de nacimiento, sexo, nacionalidad, situación administrativa, nivel educativo y estado civil.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los solos efectos de tratamiento y elaboración de las informaciones estadísticas relacionadas con los hechos ilícitos registrados en la Base de Datos de trata de seres humanos, se cederá a los respectivos servicios estadísticos de las Policías Autonómicas, con competencia integral en materia de seguridad, un número identificador, bien sea el DNI, NIE, pasaporte u otro documento identificativos correspondiente a la víctima y a los responsables penales de los hechos objeto del referido registro, de conformidad con lo establecido en el artículo 11.2.e) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, c/ Amador de los Ríos 2, 28071 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Centro de Inteligencia contra el Crimen Organizado, (CICO) calle Recoletos, 22 - 28001 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

8. FICHERO: DIETAS CICO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Dietas CICO.
a.2) Finalidad: Gestión de indemnizaciones por razón del servicio.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal adscrito al Centro de Inteligencia contra el Crimen Organizado (CICO), en comisión de servicio. Y personal de Fuerzas y Cuerpos de Seguridad del Estado y de otras Instituciones, también por comisiones de servicio relacionadas con las funciones del CICO.
b.2) Procedencia y procedimiento de recogida: De los propios interesados, en formularios y soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Los datos incluidos son:

De carácter identificativo: DNI/NIF.
De situación administrativa: Cuerpo administrativo, categoría, puesto de trabajo, y nivel.
Justificativos de la indemnización: Objeto de la comisión de servicio.

Económico-Financieros: datos bancarios, impuestos aplicables, etc.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los órganos de la Administración General de Estado competentes para la fiscalización del gasto, así como al Tribunal de Cuentas, a la Agencia Estatal de la Administración Tributaria y a las entidades de crédito en las que se proceda al abono de las dietas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, c/ Amador de los Ríos, 2, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Centro de Inteligencia contra el Crimen Organizado, (CICO) calle Recoletos, 22 - 28001 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

9. FICHERO: ANETO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ANETO.

a.2) Finalidad: Investigación policial.

a.3) Usos previstos: Registro de entrada y salida de documentación administrativa de los Centros de Cooperación Policial y Aduanera; gestión de las transmisiones o intercambios de información entre España (Guardia Civil, Cuerpo Nacional de Policía, Ertzaintza, Mossos d'Esquadra, Servicio de Vigilancia Aduanera y cualquier otro Cuerpo o Servicio que pueda ser declarado competente en virtud de acuerdo de colaboración transfronteriza suscrito por España) y el país transfronterizo (Francia, Portugal, así como cualquier otro Estado parte del Acuerdo Schengen), procedente o bien de un Cuerpo español, o bien de un Cuerpo de la contraparte; control del rendimiento y elaboración de la estadística de actividades realizadas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas implicadas en actividades delictivas e infracciones, sobre las que se solicita información o son objeto de investigación policial a nivel nacional e internacional, así como personas sobre las que se pueda necesitar un intercambio de información a nivel transfronterizo por razones humanitarias o de emergencia.

b.2) Procedencia y procedimiento de recogida: A través de las comunicaciones de correo electrónico y ordinario, fax y telefónicas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos relativos a personas en relación con el colectivo del apartado b.1):

– datos identificativos y de características personales: DNI/NIF, NIE, N.º Pasaporte, nombre y apellidos, domicilio, fecha, lugar y país de nacimiento, nombres de los padres, sexo, nacionalidad, ubicación, dirección de correo electrónico, número de teléfono, datos biométricos, fotografía, dactilogramas, cuentas bancarias, ubicación geográfica, datos sobre la estancia irregular en un territorio, número de identificación profesional de los usuarios de este fichero, así como cualquier otro que pudiera ser identificativo de la persona.

– datos relativos a objetos:

Datos identificadores de vehículos: matrícula, bastidor, tipo, marca, modelo, imágenes y comentarios.

Datos relativos a armas, joyas, medios de transporte marítimo, medios de transporte aéreo, así como cualquier otro objeto que pueda formar parte de una investigación policial.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Guardia Civil, Cuerpo Nacional de Policía, Servicio de Vigilancia Aduanera, Policías Autonómicas, Policías Locales, así como cualquier otra institución o entidad que requiera información a nivel transfronterizo por razones humanitarias o de emergencia, Cuerpos de Policía y Aduanas de la República Francesa y la República de Portugal que se encuentren en los Centros de Cooperación Policial y Aduanero, siempre dentro del marco normativo vigente.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se prevén.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, calle Amador de los Ríos, número 2, 28010 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, calle Amador de los Ríos, número 2, 28010 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

10. FICHERO: PDyRH.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: PDyRH.

a.2) Finalidad: Identificación de personas desaparecidas y cadáveres/restos humanos sin identificar, con la finalidad de poder resolver el máximo número de investigaciones relacionadas con las desapariciones de personas, buscando la colaboración entre las Fuerzas y Cuerpos de Seguridad, tanto nacionales como autonómicas.

a.3) Usos previstos: Averiguación de personas desaparecidas y la identificación de restos cadavéricos.

b) Origen de los datos:

b.1) Colectivo: Personas desaparecidas, cadáveres y restos humanos sin identificar.

b.2) Procedencia y procedimiento de recogida: Denuncias por desaparición de personas, diligencias policiales de hallazgo de cadáveres o restos humanos sin identificar y cotejo con fichero automatizado ADDNIFIL, del que se obtendrán las impresiones dactilares y fotografía de personas desaparecidas o halladas a partir de los datos identificativos que se estimen necesarios. No se admitirán consultas masivas.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

c.1.1) Datos relativos al colectivo del apartado b.1):

Datos identificativos: Nombre y apellidos, apodo, sexo, fecha y lugar de nacimiento, nombre de los progenitores, nacionalidad, número, fecha y país de expedición del documento de identificación, domicilio.

Datos relativos a la salud: Amnesia (sí/no).

Datos de características personales: Dentadura, peso, constitución física, cabello, ojos, piel, nariz, mentón, cara, presencia de gafas, tatuajes, cicatrices, lunares o verrugas, malformaciones, implantes estéticos, «piercing» o perforaciones, amputaciones.

c.1.2) Datos identificativos de las personas que denuncian la desaparición: Nombre y apellidos, fecha y lugar de nacimiento, número de documento de identificación, nacionalidad, nombre de los progenitores, domicilio, teléfono, grado de parentesco.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: Dirección General de la Policía, Dirección General de la Guardia Civil y Policías de las Comunidades Autónomas.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle López Santos, 4, 28230 Las Rozas (Madrid).

h) Nivel de seguridad exigible: Alto.

11. FICHERO: SIMASC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SIMASC.

a.2) Finalidad: Canal de comunicaciones de alertas de seguridad ciudadana a disposición de los ciudadanos, a través de un sistema de información que interactúa con los Centros de Gestión de Alertas con los que cuentan en la actualidad las unidades de 091 y 062 de las Fuerzas y Cuerpos de Seguridad del Estado.

a.3) Usos previstos: El sistema de información en movilidad para alertas de seguridad ciudadana (SIMASC) universalizará el acceso a los sistemas de aviso de alertas de seguridad ciudadana, de modo que cualquier persona con independencia de su idioma o de sus discapacidades auditivas o vocales pueda comunicarse con los servicios de gestión de alertas de las Fuerzas y Cuerpos de Seguridad del Estado del lugar en que se encuentre. Ante una situación de inseguridad comprendida en el catálogo de avisos de emergencia del sistema SIMASC, el usuario, mediante una aplicación en movilidad (app) descargada en su smartphone, podrá generar y enviar una alerta describiendo la situación y solicitando ayuda.

La plataforma recibirá la información de la alerta, procesará el mensaje y discriminará la Unidad y Cuerpo de las Fuerzas y Cuerpos de Seguridad del Estado a la que debe enviar de manera automática e inmediata la alerta. A partir de este momento se establecerá un canal de comunicación entre alertante y el Centro de Gestión de Emergencias (091 o 062) que reciba la alerta.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Ciudadanos nacionales y turistas extranjeros con independencia de su idioma o de sus discapacidades auditivas o vocales que, para comunicarse con los servicios de gestión de alertas de las Fuerzas y Cuerpos de Seguridad del Estado, decidan hacer uso de la aplicación de movilidad AlertCops publicada por el Ministerio del Interior en los markets de las operadoras telefónicas.

b.2) Procedencia y procedimiento de recogida: Los datos serán recabados mediante registro voluntario de los usuarios a través de la aplicación de movilidad AlertCopps o del Portal Web MiAlertCops publicado por el Ministerio del Interior para la gestión por los ciudadanos de la información correspondiente a sus datos personales, así como por los centros de alertas de las Fuerzas y Cuerpos de Seguridad del Estado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos de carácter identificativo y de características personales: Nombre y apellidos, DNI, NIE, NIF o pasaporte, número de teléfono, cuenta de correo electrónico, dirección postal, discapacidad auditiva (si/no) y fotografía (subida por el usuario).

– datos especialmente protegidos: Salud (grupo sanguíneo, factor RH, datos médicos generales –campo libre–).

La información recogida durante la tramitación de las alertas remitidas formará parte de la estructura del fichero, quedando esa información asociada a los usuarios que hubieran instalado la aplicación.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Centros de gestión de alertas de las Fuerzas y Cuerpos de Seguridad del Estado.

e) Transferencias internacionales de datos previstas a terceros países, con indicación en su caso, de los países de destino de los datos: No están previstas cesiones de datos internacionales a terceros países.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle López Santos, 4 y 6, 28230 Las Rozas (Madrid).

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

12. FICHERO: ACREDITACIONES.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Acreditaciones.

a.2) Finalidad: Creación de un canal de comunicación, a través de una plataforma web (portal), de datos identificativos para la posterior verificación de idoneidad, por parte de las Fuerzas y Cuerpos de Seguridad (FCS), para el acceso de personas a zonas restringidas de seguridad o de influencia para la seguridad ciudadana.

a.3) Usos previstos: El portal Acreditaciones concentrará en un único lugar los datos de las personas que deberán ser acreditadas para el acceso a zonas restringidas de seguridad o zonas de influencia para la seguridad para la seguridad ciudadana. Será la propia persona a acreditar, representante, contratante o responsable de emitir las correspondientes acreditaciones o cualquier otro interviniente con la información necesaria, siendo informado en estos casos el propio interesado de tal extremo, quien introduzca la información necesaria para que por parte de las FCS procedan a la verificación de idoneidad. Las FCS podrán interactuar con el portal mediante la descarga de los datos en él introducidos, garantizando la confidencialidad a terceros (ajenos a FCS) de los datos en él contenidos, especialmente aquellos referentes a antecedentes penales o policiales.

b) Origen de los datos:

b.1) Colectivo: Ciudadanos nacionales o extranjeros, no pertenecientes a FCS, que por razones profesionales deban tener acceso a zonas restringidas de seguridad o de influencia para la seguridad ciudadana.

b.2) Procedencia y procedimiento de recogida: Los datos serán recabados a través de un portal vía web mediante registro voluntario de los interesados, representante, contratante o responsable de emitir las correspondientes acreditaciones o por cualquier otro interviniente con la información necesaria, siendo informado, en estos casos, el propio interesado de tal extremo.

c) Estructura básica del fichero:

c.1) Descripción de los datos: Nombre y apellidos, DNI, NIE, NIF o pasaporte, fecha, localidad y provincia de nacimiento, nacionalidad, nombre de los progenitores, dirección postal de domicilio y fotografía (subida por el usuario).

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: Fuerzas y Cuerpos de Seguridad.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle López Santos, 6, 28230 Las Rozas (Madrid).

h) Nivel de seguridad exigible: Alto.

13. FICHERO: ACCESOS CETSE

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Accesos CETSE.
a.2) Finalidad: Gestionar la seguridad, verificación e identificación de las personas, vehículos y mercancías que accedan al Centro Tecnológico de Seguridad de la Secretaría de Estado de Seguridad, así como crear y mantener actualizas las correspondientes acreditaciones de acceso.
a.3) Usos previstos: Administrativo.

b) Origen de los datos:

b.1) Colectivo: Personas que accedan al Centro Tecnológico de Seguridad de la Secretaría de Estado de Seguridad.
b.2) Procedencia y procedimiento de recogida: De los propios interesados al acceder al control de visitas del Organismo. La recogida de datos es obligatoria para el acceso a las dependencias. Los datos serán recabados a través de la aplicación de registro de accesos al CETSE, directamente de la documentación aportada por las personas que pretendan acceder al edificio o a través de tarjetas automatizadas que incorporan los datos de sus titulares.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos relativos al colectivo del apartado b.1): Nombre y apellidos, DNI/NIE/pasaporte, tarjeta de identidad profesional, fecha de alta en el sistema, fecha de modificación, teléfono y extensión, localización: ausente/presente, tipo de empleado: empleado público/personal ajeno, estado: activo/baja, empresa, departamento, número de tarjeta de acceso, horario de llegada y salida, niveles de acceso autorizados.
Datos relativos a los vehículos: Matricula/s.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: No se prevén.
e) Transferencias internacionales de datos previstas a terceros países: No se prevén.
f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle Cabo López Martínez, s/n, 28048 El Pardo (Madrid).
h) Nivel de seguridad exigible: Básico.

14. FICHERO: VIDEOVIGILANCIA CETSE

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Videovigilancia CETSE.
a.2) Finalidad: Gestionar la seguridad en las instalaciones del Centro Tecnológico de Seguridad de la Secretaría de Estado de Seguridad, mediante la grabación y tratamiento automatizado de imágenes captadas en el interior y exterior del recinto.
a.3) Usos previstos: Funciones de seguridad y vigilancia.

b) Origen de los datos:

b.1) Colectivo: Personas que accedan, transiten o se encuentren en las zonas videovigiladas del Centro Tecnológico de Seguridad de la Secretaría de Estado de Seguridad.
b.2) Procedencia y procedimiento de recogida: Las imágenes son captadas y grabadas a través de los distintos sistemas de videovigilancia instalados en el edificio.

c) Estructura básica del fichero:

c.1) Descripción de los datos: Imágenes y sonido obtenidos a través de los sistemas de videovigilancia.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: No se prevén.
e) Transferencias internacionales de datos previstas a terceros países: No se prevén.
f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle Cabo López Martínez, s/n, 28048 El Pardo (Madrid).
h) Nivel de seguridad exigible: Básico.

Dirección General de la Policía.

1. FICHERO: JUIP (JEFATURA DE UNIDADES DE INTERVENCIÓN POLICIAL).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: JUIP (Jefatura de Unidades de Intervención Policial).
a.2) Finalidad: Sistema de Gestión y control de los servicios prestados por las Unidades de Intervención Policial. Ayuda para la planificación y coordinación de los movimientos y desplazamientos de las Unidades en las misiones que tienen asignadas. Concebida como una herramienta básica de trabajo y de actualización diaria, se introducen todos los servicios que realizan los funcionarios integrantes de las diferentes Unidades, de forma que en todo momento y en tiempo real se conocen los efectivos disponibles en una Unidad y un día concreto. Evaluación de la disponibilidad e inspección general de las Unidades.
a.3) Usos previstos: Gestión de los recursos humanos en el ámbito de las U.I.P,s.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todos los funcionarios con destino en U.I.P,s.
b.2) Procedencia y procedimiento de recogida: Grabación de los datos procedentes de los integrantes adscritos a las diferentes Unidades. Los funcionarios autorizados para el uso de la aplicación y siempre en el ámbito de utilización que les corresponda, es decir, en el de su destino. Nunca podrán manejar datos de otras Unidades a las que no pertenezcan.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: DNI, nombre completo, carné profesional, destino del funcionario, fecha de nacimiento, domicilio y teléfonos de contacto.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Fuerzas y Cuerpos de Seguridad, cuando tales cesiones resulten precisas para el cumplimiento de los deberes de coordinación y cooperación, según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039, Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio (acceso sólo desde la intranet y mediante control de acceso de usuarios previamente autorizados, cada

movimiento realizado en la Base de Datos es registrado, conociendo en todo momento qué usuario los ha realizado).

2. FICHERO: JUE (JEFATURA DE UNIDADES ESPECIALES).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: JUE (Jefatura de Unidades Especiales).
a.2) Finalidad: Sistema de gestión y control de servicios y recursos de las Unidades Especiales. Concebida como una herramienta básica de trabajo y de actualización diaria, se introducen todos los servicios que realizan los funcionarios integrantes de las diferentes unidades, de forma que en todo momento y en tiempo real se conoce los efectivos disponibles para una unidad dada y un día concreto, así como los servicios realizados por determinados funcionarios. También se recogen los datos pertenecientes a los animales, materiales, vehículos, intervenciones, etc., de estas unidades.
a.3) Usos previstos: Gestión de los recursos humanos en el ámbito de la JUE.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todos los miembros destinados en las Unidades Especiales.
b.2) Procedencia y procedimiento de recogida: Grabación de los datos procedentes del propio interesado. Los funcionarios autorizados para el uso de la aplicación y siempre en el ámbito de utilización que les corresponda, es decir, en el de su destino y especialidad, nunca podrán manejar datos de otras unidades o especialidades a las que no pertenezcan.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: DNI, nombre completo, carnet profesional, destino del funcionario, fecha de nacimiento, domicilio y teléfonos de contacto.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Fuerzas y Cuerpos de Seguridad, cuando tales cesiones resulten precisas para el cumplimiento de los deberes de coordinación y cooperación, según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039, Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio (acceso sólo desde la intranet y mediante control de acceso de usuarios previamente autorizados, cada movimiento realizado en la Base de Datos es registrado, conociendo en todo momento el usuario que lo ha realizado).

3. FICHERO: EUROCARGADOR.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Eurocargador.
a.2) Finalidad: Para su transmisión, por parte de la Unidad Nacional de Europol, de las aportaciones nacionales al Sistema de Información de Europol (SIE), –ubicado en la sede de Europol en La Haya (Países Bajos)– para el cumplimiento de las funciones de Europol

recogidas en el art. 5 de la Decisión del Consejo de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol), en relación con la prevención y lucha contra la delincuencia organizada, el terrorismo y otras formas de delitos graves que figuran en el anexo de la Decisión, en la medida que afecten a dos o más Estados Miembros de la Unión Europea, de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados miembros.

a.3) Usos previstos: Coordinación, tratamiento y validación por parte de la Unidad Nacional, de las aportaciones nacionales al Sistema de Información de Europol de Investigaciones e informaciones aportadas en el marco de las competencias de Europol por las Autoridades Nacionales Competentes. Se entenderá por «autoridades competentes» todos los organismos públicos existentes en los Estados miembros que sean responsables, conforme al derecho nacional, de la prevención y lucha contra los delitos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los comprendidos en el artículo 12 de la Decisión del Consejo de 6 de abril de 2009:

a) Las personas que sean sospechosas, de acuerdo con el derecho español, de haber cometido o de haber participado en un delito que sea competencia de Europol, o que hayan sido condenadas por tal delito;

b) Las personas respecto de las cuales existan indicios concretos o motivos razonables, de acuerdo con el derecho español, para presumir que cometerán delitos que son competencia de Europol.

b.2) Procedencia y procedimiento de recogida: Transferencia automática desde distintas bases de datos gestionadas por las Autoridades Nacionales competentes y remisión en formato electrónico a la Unidad Nacional de Europol de la información o investigaciones realizadas en el marco de las competencias de Europol.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: La estructura básica del fichero viene recogida en el artículo 12 de la Decisión del Consejo de 6 de abril de 2009 (Contenido del Sistema de Información de Europol): Apellido, apellido de soltera, nombre y, en su caso, alias o nombre falso utilizados; fecha y lugar de nacimiento; nacionalidad; sexo; lugar de residencia, profesión y paradero de la persona de que se trate; número de la seguridad social, permisos de conducción, documentos de identidad y datos del pasaporte, y en la medida en que sea necesario, otras características que puedan resultar útiles para su identificación, en particular rasgos físicos específicos, objetivos y permanentes, tales como los datos dactiloscópicos y el perfil de ADN (establecido a partir de la parte no codificante del ADN). Además: delitos, hechos imputados, fecha, lugar y forma de comisión (presuntamente); medios utilizados o que puedan serlo para cometer los delitos, incluida la información relativa a personas jurídicas; servicios responsables del expediente y número de referencia de este; sospecha de pertenencia a una organización delictiva; condenas, siempre que se refieran a delitos que sean competencia de Europol; parte que haya introducido los datos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando, en su caso, los destinatarios o categorías de destinatarios y transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: Al Sistema de Información de Europol y a través del mismo a las Unidades Nacionales de Europol del resto de los Estados miembros y por canal de las mismas a sus autoridades nacionales competentes, además de aquellas otras Agencias Europeas, terceros Estados y Organizaciones Internacionales con los que Europol tenga concluidos acuerdos operativos de cooperación.

e) Órgano responsable del fichero: División de Cooperación Internacional, calle Julián González Segador, sin número, 28033 Madrid.

f) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Cooperación Internacional, calle Julián González Segador, sin número, 28033 Madrid.

g) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: UCPI.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: UCPI.

a.2) Finalidad: Punto único de comunicación para el intercambio de mensajes entre las distintas Unidades de las Fuerzas y Cuerpos de Seguridad del Estado, Policías Autonómicas, Policías Locales o entidades externas (Ministerio de Justicia, Aduanas, Banco de España y cualesquiera otras susceptibles de enviar o recibir información) y la Unidad de Cooperación Internacional; y ésta a su vez con las entidades internacionales de su ámbito de competencia: Interpol, Europol y Sirene (Sistema de Información Schengen).

a.3) Usos previstos: Apoyo a la investigación policial, nacional e internacional.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas implicadas en actividades delictivas e infracciones, sobre las que se solicita información o son objeto de investigación policial a nivel nacional e internacional.

b.2) Procedencia y procedimiento de recogida: A través de las comunicaciones de correo electrónico, fax o web-mail del aplicativo.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– se recoge el nombre y apellidos, número de DNI/NIF y plantilla de destino de los usuarios de este fichero.

– existe un cuerpo de mensaje, en que se introduce información no estructurada y que posteriormente puede ser consultada.

– adjuntar archivos de todo tipo, tales como: imágenes, documentos digitales, video u audio.

– enviar y recibir mensajes de fax.

– enviar y recibir mensajes de correo electrónico.

– enviar y recibir mensajes a través de web-mail propia del aplicativo.

– maneja las entidades estructuradas de:

Genérica: Descripción y comentario.

Personas: Nombre, apellidos, DNI/NIF, fecha de nacimiento, sexo y comentarios.

Vehículos: Matrícula, bastidor, tipo, marca, modelo, color y comentarios.

– información no estructurada:

Datos de carácter personal que pueden incluirse: Datos identificativos y personales (DNI/NIF, NIE, número de pasaporte, nombre y apellidos y domicilio, fecha y lugar de nacimiento, sexo, nacionalidad, número de la Seguridad Social, número de teléfono, datos biométricos, fotografía, dactilogramas, así como cualquier otro que pudiera ser identificativo de la persona).

Datos identificadores de objetos (vehículos, cuentas bancarias, armas, joyas, etc): tipo, marca, modelo, numeración o matriculación, descripción, etc.

Datos identificadores del control: lugar, motivo, fecha, hora, duración, etc.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad del Estado, Policías Autonómicas, Policías Locales, según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, o entidades externas (Ministerio de Justicia, Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de enero, Aduanas, Banco de España y cualesquiera otras susceptibles de recibir información a la Unidad de Cooperación Internacional, según lo previsto en los artículos 36 y 33 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, artículo 94 de la Ley 58/2003, de 17 de diciembre, General Tributaria y el Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba Texto Refundido de la Ley General de la Seguridad Social).

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A entidades internacionales de su ámbito de competencia (Interpol, Europol y Sirene, Sistema de Información Shengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: División de Cooperación Internacional, calle Julián González Segador, sin número, 28033 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Cooperación Internacional, calle Julián González Segador, sin número, 28033 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

5. FICHERO: REGISTRO ELECTRÓNICO DE LA DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (ÁMBITO DEL CUERPO NACIONAL DE POLICÍA).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro Electrónico de la Dirección General de la Policía y de la Guardia Civil (Ámbito del Cuerpo Nacional de Policía).

a.2) Finalidad: Anotaciones registrales de los asientos electrónicos efectuado en el Registro para, en su caso, poder consultar la información registral de sus asientos.

a.3) Usos previstos: Recepción y remisión de las solicitudes, los escritos y las comunicaciones y de su documentación complementaria a la persona, órgano o unidad destinataria de la misma. Así como para fines estadísticos y para responder a las consultas de los propios usuarios sobre el hecho registral.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas o representantes de personas jurídicas que, a través de la sede electrónica, accedan al Registro electrónico de la Dirección General de la Policía y de la Guardia Civil (ámbito Cuerpo Nacional de Policía) creado en virtud de la Orden INT/3516/2009, de 29 de diciembre.

b.2) Procedencia y procedimiento de recogida: Por archivo de los datos introducidos en el momento de realizar el asiento.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre, apellidos, DNI/NIF, pasaporte o documento identificativo, dirección postal y electrónica, teléfono.

Datos relativos a la solicitud, escrito o comunicación presentados: fecha, hora y número de asiento registral, así como la documentación anexa que aporte la persona física o jurídica que lo presente. No se incluirán datos especialmente protegidos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Transmisión de la información y documentación a la persona, órgano o unidad destinataria de la misma.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía), Unidad de Coordinación de la Policía, C/ Miguel Ángel 5, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

6. FICHERO: SALAS 091.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Salas 091.

a.2) Finalidad: Sistema de Gestión y control de los servicios prestados por las Brigadas de Seguridad Ciudadana en su ámbito territorial. Ayuda para la planificación y coordinación de los movimientos y desplazamientos urbanos ante las demandas de los ciudadanos. Concebida como una herramienta básica de trabajo y de actualización diaria, introduciéndose todos los servicios que realizan los funcionarios integrantes de las brigadas de seguridad ciudadana, de forma que en todo momento y en tiempo real se conocen los efectivos disponibles en una Unidad y el tipo de sucesos que se atienden. Evaluación de la disponibilidad e inspección general de dichas unidades.

a.3) Usos previstos: Control y gestión operativa policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Denunciantes, víctimas, testigos e implicados en los hechos, así como las dotaciones policiales que se hacen cargo de las actuaciones.

b.2) Procedencia y procedimiento de recogida: Grabación de los datos por los operadores de la Sala, recibidos vía radio, teléfono, fax, e-mail etc., procedentes de los funcionarios adscritos a las diferentes Unidades y de las personas implicadas en los hechos y sucesos que han dado lugar a una intervención policial.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

De los funcionarios: Fecha, día y hora. Suceso. Nombre y apellidos, DNI y número de carné profesional, destino, fecha de nacimiento, así como el vehículo oficial e indicativo que tienen asignado los policías de servicio.

De los ciudadanos denunciantes, víctimas, testigos e implicados: apellidos y nombre, DNI, vehículo, domicilio y teléfono, motivo de la comisión y relación con los hechos así como con el lugar de la intervención, y/o domicilio.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Fuerzas y Cuerpos de Seguridad, cuando tales cesiones resulten precisas para el cumplimiento de los deberes de coordinación y cooperación, según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Jefatura de las plantillas policiales donde se tenga instalada esta aplicación.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

7. FICHERO: SIRENADE.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero*:* SIRENADE (Sistema de Información sobre Recién Nacidos Desaparecidos).

a.2) Finalidad: Investigación de la desaparición de bebés, neonatos y recién nacidos, cuando por razón del lugar y las circunstancias se sospeche de que se trate de delitos contra las personas, contra la libertad, las relaciones familiares, alteración del registro civil o falsificación de certificados, sin perjuicio de la concurrencia de otras infracciones comunes.

a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas (físicas o jurídicas) detenidas, imputadas, investigadas, testigos, denunciantes, familiares, víctimas y todas aquellas personas relacionadas con la desaparición en cuestión.

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal a través de denuncia, por investigaciones propias del Cuerpo Nacional de Policía, a requerimiento o solicitud de las autoridades judiciales y fiscales.

El tratamiento de los datos se someterá a las previsiones establecidas en la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, en el artículo 112 del Convenio de Aplicación del Acuerdo Schengen, de 14 de junio de 1985, y en el artículo 22 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales y administrativas.

– datos de carácter identificativo y de características personales: Nombre, filiación, sexo, DNI, pasaporte, ADN, datos biométricos, perfiles genéticos, número de la seguridad social, dirección, teléfono, imagen/voz.

– datos académicos o profesionales: Profesión.

– otros tipos de datos: todos aquellos que se deriven de las gestiones y actuaciones que se lleven a cabo en el marco de las investigaciones precisas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Órganos Judiciales. Fuerzas y Cuerpos de Seguridad y otros servicios del Cuerpo Nacional de Policía.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: a Organismos Internacionales y países

extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema de Información Schengen).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, s/n, 28043 (Madrid).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, s/n, 28043 (Madrid).

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

8. FICHERO: DIFO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: DIFO.

a.2) Finalidad: La prevención de peligros reales concretos para la seguridad pública y represión de infracciones penales mediante la identificación de autores de hechos delictivos a través de la difusión de fotogramas o imágenes obtenidas por diferentes medios de grabación, generalmente procedentes de cámaras de seguridad, que reflejan actividades delictivas en el momento de su ejecución, así como de las personas sospechosas, junto con los útiles, instrumentos o armas empleados en la perpetración de los delitos, así como la difusión de alertas de modus operandi nuevos o relevantes; todo ello de acuerdo con lo establecido en el artículo 22 de la Ley Orgánica 15/1999, de 13 de diciembre.

a.3) Usos previstos: Identificación por parte de las Fuerzas y Cuerpos de Seguridad de autores de hechos delictivos de los que solo se posee la imagen, así como la generación de alertas policiales a los agentes de seguridad sobre nuevas y complejas modalidades delictivas.

b) Origen de los datos:

b.1) Colectivo: Personas autoras o cómplices de hechos delictivos.

b.2) Procedencia y procedimiento de recogida: Los datos serán facilitados por las unidades operativas de la Policía Nacional, que han sido obtenidos en el transcurso de sus actividades de investigación de las infracciones penales.

c) Estructura básica del fichero:

c.1) Descripción de los datos: Fotogramas e imágenes obtenidos en el lugar de la comisión de un hecho delictivo; tipología delictiva, modus operandi utilizado; descripción morfológica del autor o autores de la infracción penal; identificación de la unidad policial actuante; número de atestado tramitado; nombre, apellidos, fecha de nacimiento, nacionalidad, sexo, tipo y número de documentación, número de ordinal asignado por la aplicación ARGOS, fotografía de reseña e historial delictivo de las personas identificadas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: A otras Fuerzas y Cuerpos de Seguridad, según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2 d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel de seguridad exigible: Alto

9. FICHERO: FALSIFI

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero*:* FALSIFI.

a.2) Finalidad: Registrar todos aquellos datos que aparezcan en los documentos de identidad y de viaje falsos interceptados que puedan ser considerados falsos, falsificados en la página biográfica, uso indebido, robados en blanco, obtenidos fraudulentamente, dañados, alterados en sus páginas interiores, falsificación de dispositivo electrónico auténtico conteniendo documento falso u otras alteraciones, tales como documentos y cartas de identidad, pasaportes, permisos de residencia o estancia para extranjeros y cédulas de identidad, permisos de conducir, autorizaciones de regreso, libretas de marino, visados, documentos de viaje para apátridas, refugiados y asilados, sellos de control fronterizo, billetes de pasajero, tarjetas de embarque y certificados.

a.3) Usos previstos: Investigación policial.

b) Origen de los datos:

b.1) Colectivo: Personas portadoras de documentos de identidad y de viaje falsos.

b.2) Procedencia y procedimiento de recogida: Se grabarán los datos de los documentos de identidad y de viaje falsos señalados en el apartado a.2), localizados en un control fronterizo, en cualquier otro control policial o en el marco de las investigaciones sobre redes de inmigración ilegal y falsificación de documentos.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos identificativos: Nombre, apellidos, sexo, domicilio, lugar y fecha de nacimiento, nombre de los progenitores.

Datos reales o ficticios relacionados con el documento: Fechas de expedición y caducidad, número de soporte del documento, fotografía, medidas de seguridad alteradas, sellos húmedos o secos y etiquetas adheridas.

Datos relacionados con la detección del documento de viaje o identidad falso: Control policial o fronterizo en el que se hubiera detectado, organismo en el que se hubiera realizado o intentado realizar el trámite de extranjería o la investigación policial con expresión de lugar, motivo fecha, hora y duración.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas: A otras Fuerzas y Cuerpos de Seguridad en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; a los órganos jurisdiccionales y Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países: A Organismos Internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema de Información Schengen, etc.).

f) Órgano responsable del fichero: Comisaría General de Extranjería y Fronteras, calle General Pardiñas, 90, 28006 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Extranjería y Fronteras, calle General Pardiñas, 90, 28006 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

10. FICHERO: VIDEOVIGILANCIA.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero*:* Videovigilancia.

a.2) Finalidad: Garantizar la seguridad y protección interior y exterior de las Comisarías del Cuerpo Nacional de Policía y de los edificios, instalaciones y centros vigilados por el mismo.

a.3) Usos previstos: Seguridad y protección.

b) Origen de los datos:

b.1) Colectivo: Personas que se encuentren en zonas videovigiladas de las Comisarías del Cuerpo Nacional de Policía o de los edificios, instalaciones y centros vigilados por el mismo.

b.2) Procedencia y procedimiento de recogida: Circuito cerrado de televisión.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: Imagen/voz.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: órganos judiciales, Ministerio Fiscal y otros servicios del Cuerpo Nacional de Policía para el ejercicio de las funciones legalmente encomendadas, así como a otras Fuerzas y Cuerpos de Seguridad para el ejercicio de sus funciones de protección de la seguridad pública, conforme a lo establecido en el artículo 22.2 de Ley Orgánica 15/1999, de 13 de diciembre, en cumplimiento de los principios de colaboración, mutuo auxilio y cooperación e información recíprocas que establece la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Subdirección General de Logística, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Subdirección General de Logística, calle Julián González Segador, sin número, 28043 Madrid.

i) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Dirección General de la Guardia Civil.

1. FICHERO: REGISTRO ELECTRÓNICO DE LA GUARDIA CIVIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro Electrónico de la Guardia Civil.

a.2) Finalidad: Anotaciones registrales de los asientos electrónicos efectuado en el Registro para, en su caso, poder consultar la información registral de sus asientos.

a.3) Usos previstos: Recepción y remisión de las solicitudes, los escritos y las comunicaciones y de su documentación complementaria a la persona, órgano o unidad destinataria de la misma. Así como para fines estadísticos y para responder a las consultas de los propios usuarios sobre el hecho registral.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas o representantes de personas jurídicas que, a través de la sede electrónica, accedan al Registro electrónico de la Guardia Civil, creado en virtud de la Orden INT/2936/2009, de 27 de octubre.

b.2) Procedencia y procedimiento de recogida: Por archivo de los datos introducidos en el momento de realizar el asiento.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre, apellidos, DNI/NIF, pasaporte o documento identificativo, dirección postal y electrónica, teléfono.

Datos relativos a la solicitud, escrito o comunicación presentados: fecha, hora y número de asiento registral, así como la documentación anexa que aporte la persona física o jurídica que lo presente. No se incluirán datos especialmente protegidos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Transmisión de la información y documentación a la persona, órgano o unidad destinataria de la misma.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil), Unidad de Coordinación de la Guardia Civil, C/ Guzmán el Bueno, 110, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: COS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: COS.

a.2) Finalidad: Registrar las llamadas a través de la telefonía de emergencia 062, así como las comunicaciones del Sistema de Radiocomunicaciones Digitales de Emergencias del Estado (SIRDEE).

a.3) Usos previstos: Administrativos y policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todas aquellas personas que establezcan comunicación a través de la telefonía de emergencia 062 y los componentes de la Guardia Civil que utilicen el Sistema de Radiocomunicaciones Digitales de Emergencias del Estado (SIRDEE).

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante grabación de las llamadas telefónicas o comunicaciones vía radio.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales y administrativas.

Datos de carácter identificativo: Dirección, teléfono, imagen/voz.

Otros datos de carácter identificativo: Fecha, hora, duración de la llamada y recursos/ llamada (identificación de los participantes en la comunicación).

Otros tipos de datos: Todos aquellos que se contemplen en el contenido de las comunicaciones.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Órganos judiciales. Fuerzas y Cuerpos de Seguridad y otros Servicios de la Guardia Civil en el ejercicio de sus competencias.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Guardia Civil, Estado Mayor –Sección de Operaciones–, calle Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: EXPEDIENTES PERSONAL RETIRADO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero*:* Expedientes personal retirado.

a.2) Finalidad: Gestión de los expedientes de personal retirado perteneciente a la Guardia Civil y al extinto Cuerpo de Carabineros, incluyendo aquellos expedientes tramitados en cumplimiento de lo previsto en los artículos 45 d), 49, y 97 de la Ley 42/1999, de 25 de noviembre, de Régimen del Personal de la Guardia Civil.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal retirado de la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Datos recogidos de la hoja de servicios o filiación, así como de boletines oficiales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal.

Datos de características personales: Datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad y sexo.

Datos académicos y profesionales: Formación, titulaciones, experiencia profesional.

Datos de detalle de empleo: Cuerpo/Escala, Categoría/Grado.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Órganos judiciales. Otros Órganos de la Administración del Estado para el ejercicio de competencias idénticas o que versan sobre la misma materia. Interesados legítimos en virtud de lo dispuesto en los artículos 31 y 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Guardia Civil - Jefatura de Personal, calle Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: PREVENCIÓN DE RIESGOS LABORALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Prevención de riesgos laborales.
a.2) Finalidad: Gestión informática interna de la prevención de riesgos laborales en la Guardia Civil (evaluación de riesgos, planificación preventiva, investigación de los accidentes de trabajo, formación e información en prevención de riesgos laborales, coordinación de actividades empresariales, control de los Equipos de Trabajo y de los EPI's).
a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Cuerpo de la Guardia Civil; personal de las Fuerzas Armadas; funcionarios que estén destinados en la Guardia Civil; personal laboral; personal eventual; personal de empresas concurrentes y trabajadores de las mismas cuando interactúen en el ámbito de aplicación del Real Decreto 179/2005, de 18 de febrero, sobre prevención de riesgos laborales en la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Del propio interesado y de las distintas Unidades de la Guardia Civil o relacionadas con la misma recabando la información directamente o a través de la Intranet Corporativa.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos de carácter identificativo: Nombre y apellidos, DNI/NIF, dirección, teléfono, firma.
– datos de características personales: Estado civil, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad.
– datos de circunstancias sociales: Situación militar.
– datos académicos y profesionales: Formación, titulaciones.
– datos de detalle de empleo: Cuerpo/escala, categoría/grado, puesto de trabajo.
– otros tipos de datos: Datos de prevención de riesgos laborales. Todos los relativos a la gestión integral de la prevención de riesgos laborales dentro del ámbito Guardia Civil.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Inspección de Personal y Servicios de Seguridad (Secretaría de Estado de Seguridad), Jefatura de Asistencia al Personal, Servicio de Asistencia Sanitaria y Servicio de Psicología.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se prevén.
f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle de Guzmán el Bueno 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Jefatura de Asistencia al Personal, calle de Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

5. FICHERO: USUARIOS BIBLIOTECA.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Usuarios Biblioteca.
a.2) Finalidad: Registro de usuarios de las bibliotecas existentes en los distintos centros dependientes de la Dirección General de la Guardia Civil y firma del recibo de préstamo de fondos bibliográficos.
a.3) Usos previstos: Administrativos.

b) Origen de los datos:

b.1) Colectivo: Cualquier persona que quiera hacer uso de los fondos bibliográficos, bien directamente (personal de la Guardia Civil y familiares, personal en reserva, personal retirado y familiares, o cualquier otro personal que realice su trabajo en dependencias de la Guardia Civil), o previa autorización.

b.2) Procedencia y procedimiento de recogida: Del propio interesado, mediante ficha-recibo firmado en papel y ficha informática.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, dirección, teléfono, firma.

Datos académicos y profesionales: Cuerpo/escala, categoría/grado, puesto de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Jefatura de Asistencia al Personal, calle Guzmán el Bueno 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

Secretaría General de Instituciones Penitenciarias.

1. FICHERO: PRL

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: PRL.

a.2) Finalidad y Usos previstos: Gestión de la prevención de riesgos laborales y accidentes de trabajo para el personal al servicio de la Secretaría General de Instituciones Penitenciarias. Tipificación de la finalidad: Prevención de los riesgos laborales, traslados, gestión de los servicios de prevención ajenos, estudios estadísticos, formación e información a los trabajadores en prevención de riesgos laborales, control de EPI's.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Empleados públicos penitenciarios.

b.2) Procedencia y procedimiento de recogida: Administraciones Públicas; el propio interesado o su representante legal; otras personas. Soporte utilizado para la obtención: Soporte papel y soporte informático.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, n.º de registro de personal.

Datos de características personales: Sexo, fecha de nacimiento, lugar de nacimiento, nacionalidad.

Datos de prevención de riesgos laborales: Todos los relativos a la prevención de riesgos dentro de la gestión de recursos humanos.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Entidades aseguradoras o de prevención.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: LLAMADAS TELEFÓNICAS POR CABINAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Llamadas Telefónicas por Cabinas.

a.2) Finalidad y usos previstos: Gestión de las comunicaciones telefónicas con familiares, amigos autorizados, representantes legales, autoridades y profesionales realizadas a los internos de todos los Centros Penitenciarios, llevando el registro de llamadas realizadas, al amparo de la establecido en los artículos 1 y 51 de la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas que teniendo relación de parentesco, amistad, representación legal o profesional con internos necesite acceder a los mismos para la realización de algún tipo de comunicación y cuyos datos serán facilitados por los internos de forma voluntaria, recogiéndose después los datos identificativos de las llamadas producidas por el sistema, así como los datos de los propios internos.

b.2) Procedencia y procedimiento de recogida: Del propio interesado mediante escrito entregado a las autoridades de su Centro Penitenciario por el propio interno, y de forma automática por los dispositivos TRM de comunicación telefónica recogidos en cada comunicación.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos: DNI, NIE, carnet de conducir, pasaporte o documento legal de identificación, nombre y apellidos, dirección postal y electrónica, teléfono, NIS o número de identificación sistemática del interno.

Datos de características especiales: Familiares y grado de relación con el interno.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Secretaría de Estado de Seguridad del Ministerio de Interior, de cara al cumplimiento de las funciones previstas en los artículos 12 y 13 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, C/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

3. FICHERO: SISTEMA DE INFORMACIÓN DE FARMACIAS (SIFA).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Sistema de Información de Farmacias (SIFA).
a.2) Finalidad y usos previstos: Gestión de los stocks y productos farmacéuticos de las farmacias de los Centros y de las prescripciones farmacéuticas de los internos de todos los Centros Penitenciarios.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas internas que por el hecho de estar ingresadas en prisión puedan recibir prescripciones médicas de productos farmacéuticos, cuyos datos serán facilitados por el Sistema de Información Penitenciaria, recogiéndose de forma obligatoria junto con los datos de sus circunstancias penitenciarias.
b.2) Procedencia y procedimiento de recogida: Del Sistema de Información Penitenciaria.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos: Nombre y apellidos, NIS o número de identificación sistemática del interno, localización interior.
Datos especialmente protegidos: Datos especialmente protegidos de diagnóstico y prescripción Medico Facultativa, de conformidad con el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Las que hayan de realizarse a las Administraciones Públicas Sanitarias para el ejercicio de sus competencias en la materia, en los términos permitidos en el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, C/ Alcalá, 38-40, 28014 Madrid. Teléfono: 91 335 47 92.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: GESTIÓN DE PROGRAMAS DE INTERVENCIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión de programas de intervención.
a.2) Finalidad: Controlar y gestionar todas las actividades llevadas a cabo por las ONGs, Asociaciones y Entidades Colaboradoras debidamente autorizadas en todos los Centros Penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias, así como controlar y gestionar la entrada de los voluntarios o profesionales pertenecientes a las mismas en el interior de los citados Centros.
a.3) Usos previstos:

– Nombre, razón social y responsable de ONGs, Asociaciones y Entidades Colaboradoras que intervienen en los Centros Penitenciarios.
– Ámbito territorial de actuación.
– Tipo y número de programas desarrollados en los Centros Penitenciarios según mapa de necesidades.

– Medios materiales y humanos, coste estimado y financiación de los programas a desarrollar en los Centros.

– Colaboradores autorizados a entrar en los Centros Penitenciarios: nombre y apellidos, fecha de nacimiento y nombres de los padres. Fecha de alta y de baja en la colaboración.

– Naturaleza laboral de los colaboradores: voluntario o profesional.

– Entidad aseguradora y plazos de cobertura para los colaboradores voluntarios.

– Emisión de Peticiones, Informes, Certificaciones y Acreditaciones relacionadas con el ejercicio de potestades jurídico-publicas.

– Envío de comunicaciones, en el ámbito nacional e internacional, vinculadas con el ejercicio de potestades jurídico-públicas.

– Emisión de informes estadísticos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los colaboradores, sean voluntarios o profesionales, pertenecientes a las ONGs, Asociaciones y Entidades colaboradoras que estén desarrollando alguno o algunos de los programas de intervención en los Centros Penitenciarios presentados por dichas entidades y autorizados por el Centro directivo.

b.2) Procedimiento de recogida: Fichas de adscripción presentadas por las ONGs, Asociaciones y Entidades Colaboradoras, según modelos establecidos por la Instrucción 9/2009, de 4 de noviembre, de Secretaría General de Instituciones Penitenciarias (Formularios 1 y 2), que pueden ser acompañados de Memoria de la entidad, descripción del programa a desarrollar, etc. Estos formularios cumplimentados pueden ser presentados directamente en el centro penitenciario o centro de inserción social donde se van a desarrollar el programa de intervención, o pueden ser tramitados de forma electrónica mediante cumplimentación de los «Formularios para autorizar el acceso de ONG's a los centros penitenciarios» que se encuentra en la Sede Electrónica de la Página Web del Ministerio de Interior.

b.3) Procedencia: La ONG, Asociación o Entidad Colaboradora que presenta a los colaboradores.

b.4) Soporte utilizado para la obtención: Soporte papel o soporte informático según el procedimiento elegido para la recogida de datos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Estructura:

– Datos de carácter identificativos: DNI/NIE, nombre y apellidos, dirección electrónica, teléfono.

– Datos de características personales: Fecha de nacimiento, nombre de los padres.

– Datos de detalle de empleo: Puesto de trabajo, ONG o asociación para la que trabaja.

– Datos de circunstancias sociales: Colaboración como voluntario en una ONG o asociación.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Tribunales, Jueces y Ministerio Fiscal en el ejercicio de las funciones que tienen atribuidas. Defensor del Pueblo o institución análoga de las Comunidades Autónomas que ejerzan competencias ejecutivas en materia penitenciaria. Servicios Públicos responsables de la producción de estadísticas oficiales. ONGs, Asociaciones y Entidades colaboradoras del ámbito penitenciario que lo soliciten, excluyendo los datos de carácter identificativo y personal.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. Calle Alcalá, 38-40. 28014 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias. Calle Alcalá, 38-40. 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

5. FICHERO: HISTORIA CLÍNICA DIGITALIZADA HOSPITAL PSIQUIÁTRICO ALICANTE.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Historia clínica digitalizada Hospital Psiquiátrico Alicante.

a.2) Finalidad: Valoración y seguimiento de la salud de los enfermos mentales ingresados en el hospital psiquiátrico penitenciario.

a.3) Usos previstos: Archivo de datos epidemiológicos, médico-legales, sanitario, sociales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Pacientes ingresados en el hospital psiquiátrico penitenciario de Alicante.

b.2) Procedimiento de recogida: Formularios, informes y digitalización óptica.

b.3) Procedencia: El propio interesado. Familiares y allegados. Administraciones Públicas y privadas en los términos autorizados en la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.

b.4) Soporte utilizado para la obtención: Soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Estructura:

Datos personales: datos de filiación (nombre y apellido, fecha de nacimiento, procedencia, domicilio, nombre de los padres, teléfonos de contacto…).

Datos sanitarios:

Factores de riesgo de enfermedad: Antecedentes personales, y familiares, hábitos tóxicos, conductas de riesgo...

Datos de prevención, diagnostico y tratamiento de enfermedades: Exploraciones y pruebas médicas, exploración psicológica, vacunación, actividades de enfermería. Diagnósticos y tratamientos.

Datos de laboratorio: Datos generales de laboratorio (bioquímica, hematimetría, iones…), serologías (VIH, Hepatitis, sífilis, Mantoux, tuberculosis..).

Datos médico-legales: Informes al ingreso, informes al alta, informes judiciales, informes interconsulta, informes de dependencia, partes de lesiones, informes valoración de incapacidad, informes valoración riesgo de suicidio, intoxicaciones…

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Autoridades sanitarias y judiciales, ajustándose a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, y de conformidad con lo previsto en los artículos 7.3, 7.6 y 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No hay transferencias internacionales previstas.

f) Órgano responsable del fichero: La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario y de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Hospital Psiquiátrico de Alicante. Ctra. de Madrid - Alicante, s/n. Alicante.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

6. FICHERO: VIDEOVIGILANCIA EN LOS ESTABLECIMIENTOS PENITENCIARIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Videovigilancia en los establecimientos penitenciarios.

a.2) Finalidad: Registro de imágenes obtenidas a través de los distintos sistemas de videovigilancia instalados, para el control de acceso y tránsito en los Departamentos de accesos y comunicaciones de los establecimientos penitenciarios.

a.3) Usos previstos: Videovigilancia y seguridad.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretenda obtener los datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que accedan a los establecimientos penitenciarios.

b.2) Procedencia y procedimiento de recogida: Las imágenes son captadas y grabadas a través de los distintos sistemas de videovigilancia instalados en los departamentos de accesos y comunicaciones de los establecimientos penitenciarios. El almacenamiento de dichas imágenes será como máximo de un mes de acuerdo con la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos. El tratamiento de las imágenes captadas por los dispositivos mencionados corresponderá a cada establecimiento penitenciario. Únicamente se almacenarán las imágenes correspondientes a hechos relativos a las personas y colectivos que hayan dado lugar a la incoación de algún procedimiento penal, sancionador administrativo o disciplinario, durante su tramitación y hasta la finalización de los mismos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– imágenes obtenidas a través de los sistemas de videovigilancia.

– datos relativos a la identidad de las personas o colectivos a quienes correspondan las imágenes, en su caso, si fuere preciso: Nombre, apellidos, DNI y domicilio.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Fuerzas y Cuerpos de Seguridad del Estado, Defensor del Pueblo, Ministerio Fiscal y Jueces y Tribunales en el ejercicio de las funciones que tienen atribuidas, de acuerdo con el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28004 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección de los establecimientos penitenciarios en sus respectivas sedes de ubicación.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

7. GESTIÓN DE AUTORIZACIONES Y CONTROL DE ACCESO DE PERSONAL AJENO, PROVEEDORES Y VEHÍCULOS, PARA LA REALIZACIÓN DE ACTIVIDADES EN LOS CENTROS PENITENCIARIOS..

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Gestión de autorizaciones y control de acceso de personal ajeno, proveedores y vehículos, para la realización de actividades en los Centros Penitenciarios.

a.2) Finalidad: Controlar y gestionar todas las autorizaciones de acceso de personas externas (proveedores y personal ajeno) en todos los Centros Penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias, así como controlar y gestionar la entrada y salida de las personas pertenecientes a estos colectivos al interior de los citados Centros.

a.3) Usos previstos: Labores de seguridad de los Centros Penitenciarios.

b) Origen de los datos:

b.1) Colectivo: Personas, empresas y vehículos que deban acceder al interior del Centro para el desarrollo de actividades laborales, formativas, deportivas, educacionales, etc. y personas o empresas que suministren productos al establecimiento y, por tanto, sus transportistas y vehículos deban acceder al muelle de carga y descarga.

b.2) Procedencia y procedimiento de recogida: Los datos referentes a las personas y vehículos, a las que se les conceda una autorización para acceder al interior de un Centro, así como los datos relativos a los accesos al Centro, se introducen mediante formularios cumplimentados con los datos facilitados por las personas que acceden.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

– datos de carácter identificativo: Extraídos de documentos oficiales de identificación.

– datos de características personales: Los que figuren en los documentos oficiales de identificación.

– datos relativos a la autorización de acceso: Fecha de inicio y fin de la autorización, días y horario autorizado, tipo de autorización (habitual o puntual), tipo de personal (ajeno o proveedor), empresa o entidad a la que pertenece, tipo de actividad a desarrollar en el interior del establecimiento, dependencias o lugares a los que tiene autorizado el acceso, persona encargada de recibir y acompañar en su caso y datos de vehículos autorizados al interesado (matrícula, marca, modelo, etc.), en su caso.

– datos relativos al acceso: Fecha y hora de entrada y salida, fecha y hora de paso por los distintos puntos de control, datos del vehículo (matrícula, marca, modelo, color, etc.) y, en su caso, número de tarjeta de acceso.

– datos de usuarios autorizados a acceder a la aplicación: Nombre y apellidos, NIF/NIE o número de funcionario, fechas de alta y baja en la aplicación, contraseña y perfil de usuario.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: No se prevén.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. Calle Alcalá, 38-40. 28014 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Centros Penitenciarios y Centros de Inserción Social, dependientes de la Secretaría General de Instituciones Penitenciarias.

(http://www.institucionpenitenciaria.es/web/portal/centrosPenitenciarios/localizacion.html).

h) Nivel de seguridad exigible: Básico.

Subsecretaría del Interior

1. Fichero: Base de datos unificada de personal adscrito-PERSA:

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero*:* Base de datos unificada de personal adscrito-PERSA.
a.2) Finalidad: Control interno de personal.
a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todo el personal que tenga la condición de empleado público y preste sus servicios en el ámbito de los servicios centrales del Ministerio del Interior y de las unidades adscritas a la Subsecretaría del Interior, con exclusión del personal de la Dirección General de Tráfico.
b.2) Procedencia y procedimiento de recogida: Ficha de personal, con datos proporcionados por los empleados públicos y la Administración.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre y apellidos, NIF/NIE, login.
Datos de contacto: E-mail, teléfono.
Datos de localización: Edificio, planta, despacho.
Datos relativos al puesto de trabajo: Tipo de empleado público, cargo, categoría, nivel.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Subsecretaría del Interior.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subsecretaría del Interior.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. Fichero: Gabinete Médico.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Gabinete Médico.
a.2) Finalidad: Recoger los datos identificativos y de salud de los empleados públicos, que de forma expresa lo autoricen y accedan a los servicios del Gabinete Médico de los Servicios Centrales del Ministerio del Interior.
a.3) Usos previstos: Médico.

b) Origen de los datos:

b.1) Colectivo: Empleados públicos de los Servicios Centrales del Ministerio del Interior, que accedan a los servicios del Gabinete Médico.
b.2) Procedencia y procedimiento de recogida: Datos que aporten los propios interesados al acceder al Servicio del Gabinete Médico y los que se deriven de la actividad médica de los profesionales de dicho Gabinete.

c) Estructura básica del fichero:

c.1) Descripción de los datos: DNI, nombre, apellidos, fecha de nacimiento, edad, estatura, peso, IMC, teléfono, centro de trabajo, sistema de cobertura sanitaria, número de

cotización, antecedentes familiares, antecedentes personales, alergias, vacunas, tratamiento crónico, fecha de consultas, datos de glucemia, datos de presión.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: Autoridades judiciales y Administraciones sanitarias, en los términos previstos en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Oficialía Mayor.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Oficialía Mayor, calle Amador de los Ríos, 7, 28071 Madrid.

h) Nivel de seguridad exigible: Alto.

Dirección General de Protección Civil y Emergencias

1. FICHERO: TERCEROS DE GESTIÓN ECONÓMICA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero*:* Terceros de gestión económica.

a.2) Finalidad: Control y gestión de los pagos realizados.

a.3) Usos previstos: Administrativo y de gestión.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal de la Administración, Profesores y Coordinadores de cursos de la Dirección General de Protección Civil y Emergencias, así como proveedores y servicios.

b.2) Procedencia y procedimiento de recogida: Cumplimentación de los datos del interesado mediante formularios o mediante toma directa.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: N.I.F., N.I.E., C.I.F., nombre y apellidos, domicilio, correo electrónico, cuenta bancaria (IBAN, SWIFT en su caso), número de factura e importe en número y letras.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Ministerio de Hacienda y Administraciones Públicas, para el ejercicio de sus competencias en materia de gasto público e impuestos, de acuerdo con la normativa vigente, Administración Tributaria, Tribunal de Cuentas y entidades en las que se produzca el correspondiente ingreso.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: PERSONAS EXTERNAS QUE ACCEDEN A LA DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL Y EMERGENCIAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Personas externas que acceden a la Dirección General de Protección Civil y Emergencias.
a.2) Finalidad: Control y gestión de las visitas que acceden a la Dirección General de Protección Civil y Emergencias.
a.3) Usos previstos: Administrativo y de gestión.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Ciudadanos en general.
b.2) Procedencia y procedimiento de recogida: Facilitado de los datos por el usuario de forma directa mediante la presentación del Documento Nacional de Identidad.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: N.I.F., nombre y apellidos, domicilio, nombre de la empresa a la que pertenence, teléfono.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

3. FICHERO: VIDEOVIGILANCIA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Videovigilancia.
a.2) Finalidad: Grabación y tratamiento automatizado de imágenes captadas en el interior y exterior de los recintos y edificios de la Dirección General de Protección Civil y Emergencias.
a.3) Usos previstos: Realización de labores de seguridad y vigilancia en el interior y exterior de los recintos y edificios de la Dirección General de Protección Civil y Emergencias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretenda obtener los datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas que acceden o transiten por los recintos y edificios de la Dirección General de Protección Civil y Emergencias.
b.2) Procedencia y procedimiento de recogida: Los datos registrados son recogidos por cámaras de videovigilancia mediante la captura de imágenes, previo cumplimiento del deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Imágenes en movimiento de las personas, obtenidas a través de las cámaras de videovigilancia.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando, en su caso, los destinatarios o categorías de destinatarios: Fuerzas y Cuerpos de Seguridad del Estado y Órganos Judiciales.

e) Transferencias internacionales de datos previstas a terceros países, con indicación en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias, calle Quintiliano, número 21, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

Dirección General de Tráfico.

1. FICHERO: CENTROS DE SENSIBILIZACIÓN Y REEDUCACIÓN VIAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centros de sensibilización y reeducación vial.

a.2) Finalidad: Control de los Centros de sensibilización y reeducación vial.

a.3) Usos previstos: Gestión de la competencia prevista en el artículo 5.p) del texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 339/1990, de 2 de marzo. Elaboración de estadísticas internas y públicas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares, directores, suplentes del director, asistentes del director, formadores y psicólogos-formadores de Centros de sensibilización y reeducación vial.

b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los interesados, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de los Centros de sensibilización y reeducación vial con información de sus titulares, directores, suplentes del director, ayudantes del director, formadores y psicólogos-formadores, al amparo del texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial y la Orden INT/2596/2005, de 28 de julio, por la que se regulan los Centros de sensibilización y reeducación vial: nombre y apellidos, DNI o NIE, domicilio, teléfono, perfil del formador, historial, número de registro.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

2. FICHERO: DATOS PROCEDENTES DEL CANAL TELEFÓNICO DE ATENCIÓN AL CIUDADANO DE LA DGT A TRAVÉS DE LOS NÚMEROS DE TELÉFONO HABILITADOS PARA ELLO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Datos procedentes del canal telefónico de atención al ciudadano de la DGT a través de los números de teléfono habilitados para ello.

a.2) Finalidad: Prestar un servicio de información para la realización de trámites administrativos competencia de la Dirección General de Tráfico, a través de los números de teléfono de atención al ciudadano que dicho organismo habilite para ello. Prestar un servicio de apoyo en la navegación a través del sitio web: www.dgt.es. Prestar un servicio de cita previa para los trámites administrativos relativos a conductores y vehículos que el organismo determine. Ejecución de los trámites que se establezcan como puedan ser el pago de sanciones en materia de tráfico, el pago de tasas, la identificación del conductor, comunicación de cambios de domicilio, así como cualquier otro trámite que en su momento se determine.

a.3) Usos previstos: Captación de datos para prestar un servicio de información para la realización de trámites administrativos cuya competencia corresponde a la Dirección General de Tráfico, a través del canal telefónico. Captación de datos para la tramitación de la cita previa para los trámites relativos a conductores y vehículos que el organismo determine. Pago de sanciones en materia de tráfico, a través del canal telemático y/o telefónico. Realización de otros trámites previstos por el organismo en materia de conductores y vehículos, tales como el pago de las tasas correspondientes a estos trámites, comunicación de domicilio a efectos de notificación, identificación de conductor, así como cualquier otro que se determine.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que utilizan los teléfonos habilitados para ello por la Dirección General de Tráfico.

b.2) Procedencia y procedimiento de recogida: Verbalmente por los propios interesados, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de identificación de la persona que solicita la información, cita previa, pago de tasas o sanciones: nombre, apellidos, DNI, NIE, Pasaporte, correo electrónico, Dirección Electrónica Vial (DEV), identificación de expediente sancionador. Cualquier dato procedente de los Registros de la Dirección General de Tráfico. Datos bancarios proporcionados por el interesado.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Defensor del Pueblo o entidad autonómica equivalente, Ministerio Fiscal, Jueces y Tribunales.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Secretaría General Técnica.

1. FICHERO: CONSULTAS WEB SOBRE EL REGISTRO NACIONAL DE ASOCIACIONES.

1. Fichero: Consultas Web sobre el Registro Nacional de Asociaciones.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Consultas Web sobre el Registro Nacional de Asociaciones.
a.2) Finalidad: Gestión de las consultas vía Web al Registro Nacional de Asociaciones y respuesta mediante correo electrónico.
a.3) Usos previstos: Control de las consultas realizadas por un usuario del servicio y las contestaciones, dadas con anterioridad, en el momento de redactar una nueva contestación. Estadísticas de uso del servicio y tiempo de respuesta.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Usuarios que realizan consultas vía Web al Registro Nacional de Asociaciones.
b.2) Procedencia y procedimiento de recogida: Formulario de entrada de datos en Internet.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre y apellidos, domicilio (opcional), dirección de correo electrónico a la que remitir la respuesta, consulta, respuesta, fecha y hora de la consulta y respuesta.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Cea Bermúdez, 35-37, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: INSTRUMENTA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Instrumenta.
a.2) Finalidad: Gestión del Archivo General del Ministerio de Interior.
a.3) Usos previstos: Descripción, control y recuperación de los documentos transferidos por los diferentes Órganos y Unidades del Ministerio del Interior al Archivo General del Ministerio del Interior para los siguientes fines: préstamo y servicio a los órganos productores para el ejercicio de las competencias que les son propias; servicio a los ciudadanos en el ejercicio de sus derechos; y fines históricos, científicos o estadísticos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: personas mencionadas en los expedientes conservados en los Archivos del Ministerio del Interior y cuya recuperación es de interés para los usos administrativos del Departamento, del resto de Administraciones públicas y de los usuarios que solicitan búsquedas.

b.2) Procedencia y procedimiento de recogida: A partir de los documentos y bases de datos que Órganos y Unidades transfieren al Archivo General del Ministerio del Interior.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Estructura de datos conforme a Norma Internacional de Descripción Archivística ISAD (G)/Normas Españolas de Descripción Archivística. Puede incluir todos o algunos de las Áreas y campos siguientes:

1. Identificación:

1.1 Código(s) de referencia.

1.2 Título: Cuando el título corresponde un nombre o identificación de personas, incluye datos identificativos de la misma: Apellidos y nombre, DNI, NIF, NIE u otros números de identificación personal o profesional; Puede incluir además datos de naturaleza y filiación (nombres de los progenitores, lugar de nacimiento); datos administrativos o gubernativos (infracciones administrativas; relaciones laborales con la Administración) y otros datos personales (circunstancias sociales, características personales, nacionalidad).

1.3 Fecha(s).

1.4 Nivel de descripción.

1.5 Volumen y soporte de la unidad de descripción.

2. Contexto:

2.1 Nombre de los productores: en el caso de los productores de documentos del Archivo General del Ministerio del Interior, el nombre de los productores corresponde siempre a Instituciones, nunca a personas físicas.

2.2 Historia institucional.

2.3 Historia archivística.

2.4 Forma de ingreso.

3. Contenido y estructura.

3.1 Alcance y contenido: el contenido puede consistir o incluir la referencia a una o más personas físicas, en cuyo caso incorpora datos identificativos de las mismas: Apellidos y nombre, DNI, NIF, NIE u otros números de identificación personal o profesional; Puede incluir además datos de naturaleza y filiación (nombres de los progenitores, lugar de nacimiento); datos administrativos o gubernativos (infracciones administrativas; relaciones laborales con la Administración) y otros datos personales (circunstancias sociales, características personales, nacionalidad).

3.2 Valoración, selección, eliminación.

3.3 Nuevos ingresos.

3.4 Organización.

4. Condiciones de acceso y utilización.

4.1 Condiciones de acceso.

4.2 Condiciones de reproducción.

4.3 Lengua/escritura(s) de la documentación.

4.4 Características físicas y requisitos técnicos.

4.5 Instrumentos de descripción.

5. Documentación asociada.

5.1 Existencia y localización de los originales.

5.2 Existencia y localización de copias.

5.3 Unidades de descripción relacionadas.

5.4 Nota de publicaciones.

6. Notas.
7. Control de la descripción.

7.1 Nota del Archivero: puede incluir los siguientes datos personales referentes al autor o revisor de la descripción: Nombre y apellidos, cargo.
7.2 Reglas o normas.
7.3 Fecha(s) de la(s) descripciones.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Cesiones derivadas de la ejecución de las transferencias al Archivo General de la Administración y Archivos Históricos Provinciales (Ministerio de Cultura) preceptuadas por el artículo 65.2 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, y por el Decreto 914/1969, de 8 de mayo, de creación del Archivo General de la Administración Civil.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Amador de los Ríos, 7, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: ACCARMIR.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ACCARMIR.
a.2) Finalidad y usos previstos: Tramitación de solicitudes de ciudadanos de acceso y consulta de documentos conservados en el Archivo General del Ministerio de Interior y en los archivos de gestión.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Usuarios que solicitan acceso a los fondos de los Archivos del Ministerio del Interior.
b.2) Procedencia y procedimiento de recogida: A partir del propio interesado o de su representante legal.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos del solicitante (nombre y apellidos, DNI o NIE, en su caso datos académicos y profesionales) y de contacto (dirección postal, teléfono y correo electrónico de contacto, institución en nombre de la cual se realiza la solicitud, en su caso), datos de la solicitud (motivo; datos de la investigación, en su caso; documento o documentos objeto de la solicitud); datos de tramitación (documentos que acompañan a la solicitud; fechas de solicitud, de comunicaciones y documentos relacionados con la tramitación y de resolución; estado de la solicitud y tipo de resolución recaída).
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Amador de los Ríos, 7, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

4. FICHERO: BIBLIOTECA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Biblioteca.
a.2) Finalidad y usos previstos: Relación de usuarios con derecho a préstamo externo de obras de la Biblioteca; relación de investigadores y usuarios externos de los fondos de la Biblioteca; gestión de los préstamos de libros.
b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios (del Departamento y ajenos al Departamento); investigadores, particulares y colectivos interesados; y proveedores.
b.2) Procedencia y procedimiento de recogida: Formulario.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Tratamiento de listas; Base de datos relacional.
Datos identificativos: Nombre, NIF, cargo y/o condición del solicitante (funcionario, investigador,...); destino (si funcionario), teléfono, dirección de contacto y materia sobre la que recaba información; nombre, dirección y teléfono del proveedor.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Amador de los Ríos, 7, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

5. FICHERO: DOCUMENTACIÓN (SERVICIO USUARIOS).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Documentación (Servicio Usuarios).
a.2) Finalidad y usos previstos: Recoger las demandas de información y las solicitudes de documentación recibidas en el Área de Estudios, Documentación y Publicaciones.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: El solicitante de la información o de la documentación.
b.2) Procedencia y procedimiento de recogida: Cuestionario.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Tratamiento de listas.
Tipos de datos: Nombre, cargo, condición del solicitante (particular, funcionario); destino (si funcionario), teléfono, dirección de contacto, materia sobre la que recaba información y/o documentación solicitada.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Amador de los Ríos, 7, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

6. FICHERO: PUBLICACIONES (DESTINATARIOS).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Publicaciones (Destinatarios).
a.2) Finalidad y usos previstos: Recoger información de los destinatarios y clientes de publicaciones.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas, entidades y colectivos afectados por el apartado «Finalidad y usos previstos».
b.2) Procedencia y procedimiento de recogida: Boletines de pedido y suscripción, y peticiones a través de fax o correo electrónico.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Tratamiento de listas; base de datos relacional.

– respecto a los particulares: Nombre y apellidos, NIF, domicilio, teléfono, fax, dirección de correo electrónico y dirección para el envío.
– respecto a entidades: Razón social, NIF, domicilio, teléfono, fax y dirección de correo electrónico.
– respecto a las personas de contacto en las entidades: Nombre y apellidos, teléfono y dirección de correo electrónico.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Amador de los Ríos, 7, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

7. FICHERO: ASOCIACIONES DE ÁMBITO NACIONAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Asociaciones de Ámbito Nacional.
a.2) Finalidad: Gestión del Registro Nacional de Asociaciones.
a.3) Usos previstos: Control, gestión de trámites y procedimientos seguidos para la gestión del Registro Nacional de Asociaciones.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Representantes de asociaciones.
b.2) Procedencia y procedimiento de recogida: La información se recaba a través de declaraciones y formularios que cumplimentan los propios interesados o sus representantes legales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre y apellidos, cargo en la asociación, fecha de inscripción alta del cargo, fecha de inscripción baja del cargo, fecha de asamblea.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Personas físicas y jurídicas respecto de las certificaciones del contenido de los asientos del Registro Nacional de Asociaciones previo pago de la tasa correspondiente, de conformidad con el artículo 29 de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del derecho de asociación.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Asociaciones, Documentación y Publicaciones, calle Cea Bermúdez, 35-37, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

ANEXO II

Secretaría de Estado de Seguridad

1. FICHERO: FORMACIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Formación.
a.2) Finalidad: Gestión administrativa y estadística de los cursos, seminarios, foros y jornadas de formación programados por el Centro de Inteligencia contra el Crimen Organizado y directamente vinculados con la función policial, a los que asisten miembros del Cuerpo Nacional de Policía, Cuerpo de la Guardia Civil, Dirección General de Aduanas, Policías Autonómicas y policías extranjeras. Asimismo, se correlacionan los ponentes

(jueces, fiscales, profesiones liberales, miembros de las Fuerzas y Cuerpos de seguridad, profesores universitarios).

a.3) Usos previstos: control interno del Centro de Inteligencia contra el Crimen Organizado.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Asistentes a los cursos y ponentes de los cursos (miembros de la carrera judicial, fiscal y policial, profesores liberales y profesores universitarios).

b.2) Procedencia y procedimiento de recogida: Ficha personal de cada uno de los asistentes.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Bases de datos pluritabla y relacional.

Datos de carácter identificativo: Nombre y Apellidos, DNI, Categoría, Puesto de Trabajo, Teléfono, Datos Bancarios, Importe Facturación.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevén comunicaciones de datos. A los órganos de la Administración General de Estado competentes para la fiscalización del gasto, así como al Tribunal de Cuentas, a la Agencia Estatal de la Administración Tributaria y a las entidades de crédito en las que se proceda el correspondiente abono.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: SISTEMA ESTADÍSTICO DE ANÁLISIS Y EVALUACIÓN SOBRE CRIMEN ORGANIZADO Y DROGAS SENDA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Sistema estadístico de análisis y evaluación sobre crimen organizado y drogas senda.

a.2) Finalidad: Análisis, evaluación, estudios y estadísticas en materia de drogas, de precursores de éstas, sobre otras formas de crimen organizado y sobre bienes destinados al Fondo de bienes decomisados.

a.3) Usos previstos: Usos por parte del Centro de Inteligencia contra el Crimen Organizado, las Fuerzas y Cuerpos de Seguridad y Servicios con competencia en estas materias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas que figuren en las diligencias policiales relacionadas con el tráfico ilícito de drogas y otras formas de crimen organizado y con bienes destinados al Fondo de bienes decomisados. Personas físicas y representantes de personas jurídicas, inscritas como operadores de precursores de drogas.

b.2) Procedencia y procedimiento de recogida: La información es facilitada por el Centro de Inteligencia contra el Crimen Organizado, las Fuerzas y Cuerpos de Seguridad y otros Servicios competentes en materia de drogas y otras formas de crimen organizado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Fichero relacional entre actuaciones policiales en materia de drogas y otras formas de crimen organizado, consumos prohibidos, decomisos, detenidos, denunciados, fallecidos, drogas, precursores, objetos y dinero. Los datos de carácter personal son los figuren en las diligencias policiales, y pueden referirse a nombre, DNI o pasaporte, fecha de nacimiento, lugar de nacimiento, domicilio, profesión, nombre del padre y de la madre, nacionalidad y sexo.

Respecto a los operadores de precursores de drogas, pueden figurar los siguientes datos de carácter personal: nombre, apellidos, razón social, CIF/NIF, domicilio, teléfono, fax, correo electrónico.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A Organismos internacionales y países extranjeros en aplicación de tratados o convenios en los que España sea parte.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: SISTEMA DE REGISTRO DE INVESTIGACIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Sistema de registro de investigaciones.

a.2) Finalidad: Detección, prevención y coordinación de investigaciones coincidentes entre las Fuerzas y Cuerpos de Seguridad y otros Organismos o Servicios con competencias en materia de drogas y de otras formas de crimen organizado.

a.3) Usos previstos: Usos por parte del Centro de Inteligencia contra el Crimen Organizado, las Fuerzas y Cuerpos de Seguridad y Servicios con competencia en estas materias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas y organizaciones que figuren en las investigaciones policiales relacionadas con el tráfico de drogas y de otras formas de crimen organizado.

b.2) Procedencia y procedimiento de recogida: La información es facilitada por las Fuerzas y Cuerpos de Seguridad y otros Servicios competentes en materia de drogas y de otras formas de crimen organizado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Fichero relacional entre datos de investigaciones policiales en materia de drogas, blanqueo de capitales y delitos conexos a los anteriores, u otras formas de crimen organizado, con personas físicas, personas jurídicas, cuentas bancarias, bienes inmuebles, teléfonos, medios de transporte, domicilios, correos electrónicos y páginas web. Los datos de carácter personal son los figuren en las investigaciones policiales y que pueden referirse a nombre, DNI o pasaporte, fecha de nacimiento, lugar de nacimiento, profesión, nombre del padre y de la madre, nacionalidad, lugar de residencia y sexo.

Figura, asimismo, respecto de cada investigación concreta, el nombre de la operación, número de referencia de origen, Unidad investigadora y responsable policial, y número de referencia en el Sistema de Registro de Investigaciones.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad en virtud de lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A Organismos internacionales y países extranjeros en aplicación de tratados o convenios en los que España sea parte.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: CONTROL PRESUPUESTARIO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Control presupuestario.

a.2) Finalidad: Seguimiento y control de los gastos e inversiones realizadas a partir de la asignación presupuestaria correspondiente al ejercicio económico.

a.3) Usos previstos: Control de expedientes y recursos presupuestarios.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: personal administrativo que gestiona o propone gastos con cargo a los presupuestos del Centro de Inteligencia contra el Crimen Organizado. Personal perteneciente a las empresas con las que este Centro contrae compromisos relativos a los expedientes de contratación.

b.2) Procedencia y procedimiento de recogida: Correo electrónico, correo postal, presentación física de documentos, fax y contactos telefónicos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Bases de datos pluritabla y documental.

Datos de carácter identificativo: Nombre y Apellidos, cargo, teléfono, fax, dirección postal y electrónica. Se almacena el documento completo.

Naturaleza de los expedientes: suministros, servicios, obras, colaboración, etc.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los órganos de la Administración General de Estado

competentes para la fiscalización del gasto, así como al Tribunal de Cuentas, a la Agencia Estatal de la Administración Tributaria y a las entidades de crédito en las que se proceda el correspondiente abono.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

5. FICHERO: QUEJAS Y SUGERENCIAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Quejas y Sugerencias.

a.2) Finalidad: Recogida y tratamiento de datos en los libros de quejas y sugerencias existentes en las dependencias de la Dirección General de la Policía y en la Dirección General de la Guardia Civil, y en aquellos otros documentos, cualesquiera que fuere su forma, que sean remitidos por los ciudadanos o presentados para ello, en las distintas Administraciones Públicas, de acuerdo con los criterios fijados por la Instrucción n.º 10/1997, de 9 de junio, de la Secretaría de Estado de Seguridad.

a.3) Usos previstos: Control y supervisión de los datos reflejados en los distintos documentos, así como en las hojas de los referidos libros, por parte de la Subdirección General de Inspección y Personal de Servicios de Seguridad.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que han formulado quejas o sugerencias en las hojas de los correspondientes libros habilitados al efecto en las dependencias de la Dirección General de la Policía y de la Dirección General de la Guardia Civil, así como aquéllas otras que las formalicen ante las distintas Administraciones Públicas o directamente las remitan por sí mismas con el referido objeto. Funcionarios afectados por las quejas.

b.2) Procedencia y procedimiento de recogida: Extrayéndolos de los distintos documentos e impresos formalizados enviados a la Subdirección General de Inspección de Personal y Servicios de Seguridad por la Dirección General de la Policía y por la Dirección General de la Guardia Civil, así como aquellos procedentes del resto de las Administraciones Públicas y de los remitidos por los particulares. Extrayéndolos de los documentos elaborados por los funcionarios afectados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre, apellidos, domicilio, documento nacional de identidad, firma, rúbrica del interesado, así como los datos referidos a la concreta reclamación planteada. Nombre y apellidos de funcionarios afectados.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Autoridades Judiciales y Ministerio Fiscal, de oficio ante un hecho que reviste los caracteres de delito, o previa solicitud de las citadas Autoridades, y otros órganos de la Administración, de conformidad con lo establecido en el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad. Inspección de Personal y Servicios de Seguridad. C/ Cea Bermúdez, 35-37, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

6. FICHERO: CONTROL DE VISITAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Control de Visitas.
a.2) Finalidad: Gestionar la seguridad y control de los accesos de personas y vehículos a la sede del Ministerio del Interior en las Rozas de Madrid (Madrid).
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que accedan a dicho recinto.
b.2) Procedencia y procedimiento de recogida: Directamente de la documentación aportada por las personas que pretenden acceder al edificio. Soporte utilizado para la obtención: Soporte informático.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:
c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, imagen, dirección postal, teléfono y vehículo del interesado.
Datos de características personales: Fecha y lugar de nacimiento, sexo y nacionalidad.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevén cesiones de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, C/ Amador de los Ríos, 2, 28010 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

7. FICHERO: INT-SAIP.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: INT-SAIP.
a.2) Finalidad: Cooperar con la Administración de Justicia mediante la identificación genética de vestigios biológicos y la identificación de muestras de origen conocido, en investigaciones realizadas por el Ministerio del Interior.
a.3) Usos previstos: Investigación y averiguación de delitos, así como la comprobación del delito y averiguación del delincuente según la Ley de Enjuiciamiento Criminal, de conformidad con lo previsto en la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas que determinen los Jueces y Tribunales, en el ejercicio de las funciones que tienen legalmente atribuidas, las relacionadas con restos humanos o vestigios que constituyan objeto de análisis, las relacionadas con hechos investigados que voluntariamente se sometan al tratamiento y los sospechosos, detenidos o imputados, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados.

b.2) Procedencia y procedimiento de recogida: El propio interesado, otras personas físicas distintas del afectado (con sujeción a lo expresado en el párrafo anterior y al amparo de la Ley de Enjuiciamiento Criminal), o su representante y las administraciones públicas, mediante formulario, transmisión electrónica de datos/Internet y diversos análisis de laboratorio ya sea en soporte papel, vía telemática o soporte informático o magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales.

Datos relativos a la salud: perfiles genéticos obtenidos de muestras biológicas, los cuales proporcionen, exclusivamente, información genética reveladora de la identidad de la persona, sexo, ancestralidad y rasgos físicos externos, sin que de dichos perfiles se extraiga información relativa a la salud de las personas.

Datos de carácter identificativo: DNI/NIF/Pasaporte, nombre y apellidos, dirección postal, teléfono, y datos del perfil genético con valor identificativo.

Datos de características personales: Datos de filiación, datos familiares, fecha y lugar de nacimiento, edad, sexo y nacionalidad.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: De conformidad con lo establecido en la Ley Orgánica 10/2007, de 8 de octubre:

– Los datos sólo podrán utilizarse por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas del Cuerpo Nacional de Policía y de la Guardia Civil en el ejercicio de sus funciones; así como por las Autoridades Judiciales y Fiscales, en la investigación de los delitos enumerados en la citada Ley Orgánica.

– Los datos podrán cederse a las Policías Autonómicas con competencias en materia de Seguridad Ciudadana que sólo los utilizarán para la investigación de los delitos enumerados en la citada Ley Orgánica; y al Centro Nacional de Inteligencia para la prevención de tales delitos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A las Autoridades Judiciales, Fiscales o Policiales de terceros países de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes, de conformidad con lo establecido en la Ley Orgánica 10/2007, de 8 de octubre.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, C/ López Santos, n.º 6, 28230 Las Rozas (Madrid).
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

8. FICHERO: INT-FÉNIX.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: INT-FÉNIX.
a.2) Finalidad: Identificación genética de personas desaparecidas y cadáveres sin identificar, con la finalidad científica, de interés público, social y judicial, en investigaciones del Ministerio del Interior.
a.3) Usos previstos: Procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas, así como la comprobación del delitos y averiguación del delincuente según la Ley de Enjuiciamiento Criminal, de conformidad con lo previsto en la Ley Orgánica 10/2007, de 8 de octubre.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas genéticamente relacionadas con restos humanos, las desaparecidas, las genéticamente relacionadas con desaparecidos, y las que determinen los Jueces y Tribunales en el uso de sus atribuciones.
b.2) Procedencia y procedimiento de recogida: Actividades de investigación e identificación de restos humanos realizadas por el Ministerio del Interior, así como toma de muestras referidas en el apartado anterior para los correspondientes cotejos identificativos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la salud: perfiles genéticos; obtenidos de muestras biológicas, los cuales proporcionen, exclusivamente, información genética reveladora de la identidad de la persona, sexo, ancestralidad y rasgos físicos externos, sin que de dichos perfiles se extraiga información relativa a la salud de las personas.
Datos de carácter identificativo: DNI/NIF/Pasaporte, nombre y apellidos, dirección postal, teléfono, descripción, rasgos fisonómicos, antropológicos y datos del perfil genético con valor identificativo.
Datos de características personales: Datos de filiación, datos familiares, fecha y lugar de nacimiento, edad, sexo y nacionalidad, lugares de estancia habitual.
De las personas que se aporten datos para cotejos identificativos se obtendrán e incluirán los datos que resulten precisos al fin que se pretende.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: De conformidad con lo establecido en la Ley Orgánica 10/2007, de 8 de octubre:

– Los datos sólo podrán utilizarse por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas del Cuerpo Nacional de Policía y de la Guardia Civil en el ejercicio de sus funciones; así como por las Autoridades Judiciales y Fiscales; quienes en todos los casos, sólo los utilizarán en la investigación de los casos de identificación para los que fueron obtenidos.
– Los datos podrán cederse a las Policías Autonómicas con competencias en materia de Seguridad Ciudadana que sólo los utilizarán para la investigación de los casos de

identificación de cadáveres o averiguación de personas desaparecidas, para los que fueron obtenidos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A las Autoridades Judiciales, Fiscales o Policiales de terceros países de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes, de conformidad con lo establecido en la Ley Orgánica 10/2007, de 8 de octubre.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad. C/ López Santos, n.º 6 – 28230 Las Rozas (Madrid).

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

9. FICHERO: SISTEMA ESTADÍSTICO DE CRIMINALIDAD (SEC).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Sistema estadístico de criminalidad (SEC).

a.2) Finalidad: Tener un conocimiento más profundo de los factores que inciden en la seguridad ciudadana, derivado del caudal de información que genera la actividad delictiva e infractora, así como estructurar, de acuerdo con criterios rigurosos y técnicos, la obtención, explotación y difusión de datos estadísticos relacionados con las infracciones penales y contra las leyes de seguridad ciudadana.

a.3) Usos previstos: Fines estadísticos, con objeto de articular en cada momento las políticas de seguridad más adecuadas y establecer los planes de acción preventivos que en cada ámbito territorial correspondan.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Denunciantes y víctimas de infracciones contempladas en las leyes penales y de protección de la seguridad ciudadana, así como las personas sobre las que, presuntamente, pudiera recaer alguna responsabilidad por las indicadas infracciones.

b.2) Procedencia y procedimiento de recogida: Los datos procederán de las diligencias instruidas con ocasión de actuaciones policiales, reseñas de detenidos, denuncias recibidas a través de las propias Fuerzas y Cuerpos de Seguridad del Estado y diferentes Cuerpos de Policía dependientes de las Comunidades Autónomas y Corporaciones Locales con las que se establezcan acuerdos de colaboración.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Sobre la base del desglose de las diferentes infracciones, de conformidad con la tipificación legal de las mismas, se recogerán los siguientes datos personales, asociados a ellas:

Datos de carácter identificativo: DNI/NIF/pasaporte/y otros documentos identificativos.

Datos de características personales: Fecha de nacimiento, sexo, nacionalidad, lugar de residencia y estado civil.

Datos relativos a la comisión de infracciones penales contra las leyes de Seguridad Ciudadana: Implicación y consumo de drogas y/o alcohol por parte de los responsables de la comisión de infracciones penales.

Datos académicos y profesionales: Titulación académica y situación ocupacional/laboral.

Datos de circunstancias sociales: Respecto a los ciudadanos que no posean la nacionalidad española, su situación administrativa en España, medio utilizado para su entrada en territorio nacional y motivo de su estancia en España.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los solos efectos de tratamiento y elaboración de las informaciones estadísticas relacionadas con los hechos ilícitos registrados en el Sistema Estadístico de Criminalidad, se cederá a los respectivos servicios estadísticos de las Policías Autonómicas, con competencia integral en materia de seguridad, un número identificador, bien sea el DNI, NIE, pasaporte u otro documento identificativo correspondiente a la víctima, el denunciante o el autor de los hechos objeto del referido registro.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, calle Amador de los Ríos, 2, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, Gabinete de Estudios de Seguridad Interior, paseo de la Castellana, 64, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

10. FICHERO: BDSN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: BDSN.

a.2) Finalidad: Contribuir a la preservación del orden y la seguridad públicos, incluida la seguridad del Estado. Identificar a los propietarios de vehículos y objetos robados para casos de recuperación de éstos.

a.3) Usos previstos: Gestión de la Base de Datos de Señalamientos Nacionales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas buscadas para extradición; personas requisitoriadas; extranjeros con entrada y permanencia prohibidas en territorio nacional; personas desaparecidas; incursos en procedimientos penales; y, en general, personas de las que se tengan indicios reales de que pueden suponer una amenaza para la seguridad ciudadana o del Estado.

b.2) Procedencia y procedimiento de recogida: Fuerzas y Cuerpos de Seguridad, en aplicación de la Ley Orgánica 2/1986, de 13 de marzo, Autoridades judiciales, los propios afectados o sus representantes legales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

En relación con el colectivo del apartado b.1): DNI/NIF; nombre y apellidos; dirección, teléfono; características físicas o antropométricas; datos de filiación; fecha/lugar de nacimiento; sexo; nacionalidad; alias y falsas identificaciones.

En relación con los vehículos sustraídos y recuperados: Matrícula; número de bastidor.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: Dirección General de Tráfico en lo que respecta a los datos de vehículos sustraídos y recuperados; Dirección General de la Policía, Dirección General de la Guardia Civil, Servicio de Vigilancia Aduanera, Asuntos Consulares, Policías Autonómicas y Policías Locales, Jueces y Magistrados, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre, así como en los artículos 3 y 4 de la Ley Orgánica 2/1986, de 13 de marzo; Sistema de Registro de Nombre de Pasajeros (PNR), en virtud de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros

(PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

e) Transferencias internacionales de datos previstas a terceros países: Las que se realizarán en el ámbito del Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985; las realizadas en virtud del Protocolo Operativo firmado por el Secretario de Estado de Seguridad y el Embajador de los Estados Unidos en España, el 17 de septiembre de 2007, para el intercambio de información relativa a individuos pertenecientes a grupos u organizaciones terroristas entre el Terrorist Screening Center (TSC) –perteneciente a la Oficina Federal de Investigación de los Estados Unidos de América (FBI)– y el Centro Nacional de Coordinación Antiterrorista (CNCA), cuyas funciones y competencias, actualmente han sido asumidas por el Centro de Inteligencia Contra el Terrorismo y Crimen Organizado (CITCO), a través de una base de datos alimentada con información aportada por el Terrorist Screening Center (TSC), así como por los datos que periódicamente se solicitan a la Base de Datos de Señalamientos Nacionales (BDSN) y a la Secretaría General de Instituciones Penitenciarias.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle Cabo López Martínez, s/n, 28048 El Pardo (Madrid).

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

11. FICHERO: N.SIS II/SIRENE II.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: N.SIS II/SIRENE II.

a.2) Finalidad: Preservar el orden y la seguridad públicos, incluida la seguridad del Estado, y la aplicación de las disposiciones del Reglamento (CE) número 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de información de Schengen de segunda generación (SIS II), así como de la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de información de Schengen de segunda generación (SIS II).

a.3) Usos previstos: Gestionar la parte española del Sistema de Información de Schengen, respecto de personas y objetos recogidos en el Reglamento (CE) número 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, así como en la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas cuyas características corresponden a las señaladas en el Reglamento (CE) número 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, así como de la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007.

b.2) Procedencia y procedimiento de recogida: A partir de comunicaciones judiciales o policiales, al amparo de lo establecido en la Ley Orgánica 2/1986, de 13 de marzo, así como los provenientes de los países previstos en el ámbito de aplicación del Reglamento (CE) número 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, así como de la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– en relación con el colectivo del apartado b.1):

Datos identificativos y de características personales: nombre y apellidos, nombre y apellidos de nacimiento, nombre y apellidos anteriores y alias, registrados por separado en su caso; rasgos físicos particulares, objetivos e inalterables; lugar y la fecha de nacimiento; sexo; fotografías; impresiones dactilares; nacionalidad o nacionalidades.

Otros tipos de datos: indicación de que las personas están armadas, son violentas o han huido; motivo de la descripción; autoridad informadora; referencia a la decisión que da lugar a la introducción de la descripción; conducta que debe observarse; conexión o conexiones con otras descripciones introducidas en SIS II; tipo de delito.

– datos relativos a vehículos: Matrícula; número de bastidor.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Dirección General de la Policía, Dirección General de la Policía de la Guardia Civil, Servicio de Vigilancia Aduanera, Asuntos Consulares, Policías Autonómicas y Policías Locales, Dirección General de Tráfico, Jueces y Magistrados, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre, y en los artículos 3 y 4 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: Aquellos países previstos en el ámbito de aplicación del Reglamento (CE) número 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, así como de la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, calle López Santos, 6, 28230 Las Rozas (Madrid).

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

12. FICHERO: REGISTRO GENERAL DE OPERADORES DE SUSTANCIAS QUÍMICAS CATALOGADAS (RESUCA).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

a.2) Finalidad: Inscripción de las personas físicas y jurídicas que pretendan poner en el mercado sustancias químicas de las categorías 1 y/o 2 del anexo I del Reglamento (CE) N.º 273/2004 del Parlamento Europeo y del Consejo, de 11 de febrero de 2004, sobre precursores de drogas. Registro de las licencias de actividad necesarias para el desarrollo de actividades que tengan por objeto sustancias catalogadas de la categoría 1 del anexo I del Reglamento (CE) N.º 273/2004. Control administrativo de sustancias químicas catalogadas y no catalogadas, derivado de la aplicación de la Ley 4/2009, de 15 de junio, de control de precursores de drogas.

a.3) Usos previstos: Control de las actividades relacionadas con las sustancias químicas citadas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los sujetos obligados serán las personas físicas o jurídicas que pretendan poner en el mercado sustancias químicas catalogadas de las categorías 1 y 2 del anexo I del Reglamento (CE) N.º 273/2004.

b.2) Procedencia y procedimiento de recogida: A partir de la documentación aportada por los sujetos obligados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Fichero multibase.

Datos identificativos: nombre, apellidos, razón social, CIF/NIF, domicilio, teléfono, fax, correo electrónico.

Datos profesionales: actividades que realizan, número de inscripción en el registro, número de licencia de actividad, sustancias que emplean, productos elaborados.

Datos relativos a infracciones cometidas en el desarrollo de dichas actividades y a los procedimientos sancionadores instruidos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las autoridades competentes aplicación de la Ley 4/2009, de 15 de junio, y de su normativa de desarrollo. Fuerzas y Cuerpos de Seguridad, a tenor de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A Organismos internacionales y países extranjeros en aplicación de tratados o convenios en los que España sea parte.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, Centro de Inteligencia contra el Crimen Organizado, C/ Recoletos, 22, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

13. FICHERO: VIOLENCIA DOMÉSTICA Y DE GÉNERO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Violencia doméstica y de género.

a.2) Finalidad: Mejorar la eficacia en la protección de las víctimas de violencia doméstica y de género; facilitar el seguimiento de las circunstancias de riesgo que concurren en ellas; alertar de su evolución, permitiendo que se adopten las medidas de protección adecuadas; y prevenir el riesgo de nuevas agresiones.

a.3) Usos previstos: Protección a las víctimas; prevención de infracciones penales relacionadas con la violencia doméstica y de género y tratamiento penitenciario a los agresores. Asimismo perseguirá como aspecto complementario fines estadísticos y asistenciales.

b) Origen de los datos:

b.1) Colectivo: Las personas que sean víctimas de hechos susceptibles de ser tipificados como violencia doméstica y de género y las personas incursas en procedimientos judiciales e investigaciones policiales por hechos relacionados con la violencia doméstica y de género.

b.2) Procedencia y procedimiento de recogida: Serán competentes para introducir y modificar los datos, las Fuerzas y Cuerpos de Seguridad, las Administraciones Penitenciarias, las Delegaciones y Subdelegaciones del Gobierno, los órganos judiciales del orden penal, los Juzgados de violencia sobre la mujer, las Unidades de Valoración Forense integral de los Institutos de Medicina Legal del Ministerio de Justicia y de las Comunidades Autónomas, el Ministerio Fiscal, los servicios asistenciales y sanitarios de las diferentes Administraciones Públicas, los puntos de coordinación de las órdenes de protección de violencia doméstica y de género y las oficinas de atención a la víctima del delito de las Comunidades Autónomas en relación a las materias de su competencia y en su ámbito territorial.

Los datos procederán de las denuncias presentadas ante las Fuerzas y Cuerpos de Seguridad, de los atestados policiales, de las resoluciones dictadas por los órganos judiciales y penitenciarios y de los expedientes que cursen los diferentes servicios y órganos que presten asistencia a las víctimas.

Conservación y cancelación de datos: Con arreglo a lo dispuesto en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de diciembre, se cancelarán los datos cuando:

Se archiven las denuncias presentadas.

Finalice la vigencia de la medida judicial de protección (ya se trate de medida cautelar o cumplimiento de condena, en centro penitenciario o en medida alternativa).

Acceso a la información de la base de datos de carácter personal:

1. El acceso a la información contenida en la base de datos quedará limitado a los sujetos y finalidades siguientes:

Los órganos judiciales del orden penal y los Juzgados de violencia sobre la mujer podrán acceder a la información que precisen para la tramitación de causas penales, así como para la adopción, modificación, ejecución y seguimiento de medidas de protección de dichas víctimas, a través del correspondiente secretario judicial o de un funcionario adscrito a la oficina judicial por él designado.

El Ministerio Fiscal podrá acceder a la información precisa para la tramitación de causas penales, así como para la adopción, modificación, ejecución y seguimiento de las medidas de protección de dichas víctimas, a través de los fiscales destinados en las fiscalías de los órganos jurisdiccionales competentes.

La policía judicial y las unidades policiales especializadas en violencia de género podrán acceder a la información necesaria para el desarrollo de las actuaciones que le estén encomendadas en relación con la persecución y seguimiento de las conductas que tienen acceso a esta base de datos y para el control y ejecución de las medidas de protección a las víctimas, a través de los funcionarios autorizados que desempeñen estas funciones.

Las Administraciones penitenciarias competentes, a través de los Directores de los Centros Penitenciarios o de los Centros de Inserción Social, podrán acceder a la información relativa a los quebrantamientos de condena, medidas de seguridad o medidas cautelares que se produzcan durante los permisos penitenciarios o durante la situación de libertad condicional de los internos que se encuentren sujetos a medidas judiciales de alejamiento o prohibición de comunicación con la víctima de violencia doméstica o de género. Así como los hechos en los que puedan estar involucrados los condenados a medidas alternativas tales como trabajo en beneficio de la comunidad, medidas de seguridad privativas o no de libertad, suspensiones de condena, sustituciones de condena y localización permanente.

Las Delegaciones y Subdelegaciones del Gobierno podrán acceder a la información necesaria para garantizar el efectivo cumplimiento de las medidas de protección, provisionales o definitivas, adoptadas por los órganos jurisdiccionales, a través del responsable de la unidad de protección a las víctimas de la violencia doméstica o de género o, en su caso, a través de las personas designadas por dicho responsable.

Las Unidades de Valoración Forense Integral de los Institutos de Medicina Legal del Ministerio de Justicia y las Comunidades Autónomas, a través de su responsable o de las personas designadas por el mismo, podrán acceder a la información necesaria para el desarrollo de sus actuaciones médico-psicológicas y sociales de una acción presuntamente delictiva.

Las Comunidades Autónomas, exclusivamente en el ámbito de las competencias de protección de las víctimas de violencia doméstica o de género en su territorio, podrán acceder a la información necesaria para el cumplimiento de sus funciones de información y asistencia social integral de las víctimas, a través del responsable, o de las personas designadas por dicho responsable, de los siguientes servicios:

Los servicios asistenciales.

Los puntos de coordinación de las órdenes de protección de violencia doméstica y de género.

Las oficinas de atención a la víctima del delito.

Los servicios sanitarios.

Las Entidades Locales, exclusivamente en el ámbito de las competencias de protección de las víctimas de violencia doméstica o de género en su territorio, podrán acceder a la información necesaria para el cumplimiento de sus funciones de información y asistencia

social integral de las víctimas, a través del responsable de los servicios asistenciales o de las personas designadas por dicho responsable.

2. El acceso a los datos del Registro Central se llevará a cabo telemáticamente, mediante procedimientos de identificación y autentificación. El sistema de acceso deberá dejar constancia de la identidad de los usuarios que accedan, de los datos consultados, del momento de acceso y del motivo de la consulta.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales relacionadas con la violencia doméstica y de género: Infracciones y antecedentes penales de los presuntos autores y situación penitenciaria de los mismos, relativa a la concesión de permisos o la puesta en libertad (condicional o definitiva) de los internos que se encuentren sujetos a medidas judiciales de alejamiento o prohibición de comunicación con la víctima. Así como todos aquellos que se encuentren condenados a penas o medidas alternativas diferentes al ingreso en prisión.

Datos de carácter identificativo: DNI/NIF/pasaporte/, así como otros documentos de identidad, fotografía, domicilios, teléfonos y correo electrónico.

Datos de características personales: Datos de filiación, familiares, fecha y lugar de nacimiento, sexo, nacionalidad, situación laboral, profesión, nivel educativo y estado civil.

Datos de carácter asistencial y de apoyo a las víctimas que figuren en los expedientes que elaboren los diferentes servicios y órganos que presten servicio a las víctimas de violencia de género, tales como el tipo de ayuda que la víctima reciba, utilización de casas de acogida, etc.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Instituciones y Organismos relacionadas en el apartado b.2., de conformidad con lo dispuesto en los artículos 11 y 21 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países: Organismos Internacionales y países extranjeros en los términos establecidos en los Tratados, Convenios o acuerdos (bilaterales o multilaterales) en los que España sea parte.

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad, calle Amador de los Ríos, 2, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad, calle Amador de los Ríos, 2, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

14. FICHERO: PATRONATO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Patronato.

a.2) Finalidad: Gestión de la contabilidad y financiación de las viviendas que se integraban en el Patronato de viviendas de la Guardia Civil.

a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas y empresas que tengan relaciones con el extinto Patronato de Viviendas de la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Aportados a través de formularios por los propios interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos de identificación personal (nombre, apellidos, domicilio) y datos económico-financiero, incluyendo, en su caso, datos sobre créditos.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la Administración Tributaria, en virtud de la Ley 40/1998, de 9 de diciembre, del Impuesto de la Renta de las Personas Físicas.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Comisión liquidadora del Patronato de Viviendas de la Guardia Civil. Subdirección General de Planificación y Gestión de Infraestructuras y Medios para la Seguridad.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Comisión Liquidadora del Patronato de Viviendas de la Guardia Civil. Calle Chile, 18. Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

15. FICHERO: S.A.I.D.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: S.A.I.D.
a.2) Finalidad: Cotejo e incorporación de reseñas decadactilares de detenidos al sistema de identificación dactilar. Cotejo de huellas anónimas reveladas en el lugar del hecho para la identificación de detenidos.
a.3) Usos previstos: Investigaciones policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas detenidas por infracciones penales y extranjeros detenidos en aplicación de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.
b.2) Procedencia y procedimiento de recogida: La información es grabada por los gestores a partir de las reseñas inspecciones oculares o asuntos investigados por las Direcciones Generales de la Policía y de la Guardia Civil.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y de características personales (documento nacional de identidad/número de identificación fiscal, nombre y apellidos, huella, imagen, número de registro, fecha y lugar de nacimiento, sexo).
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad, según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Secretaría de Estado de Seguridad. Calle Amador de los Ríos, 2, 28046 Madrid.

g) Servicio o unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría de Estado de Seguridad. Calle Amador de los Ríos, 2, 28046 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Dirección General de la Policía.

1. FICHERO: ACCESOS EDIFICIOS POLICIALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Accesos edificios policiales.

a.2) Finalidad: Gestionar la seguridad de un centro o edificio policial, a través de la identificación de las personas y vehículos y el control de acceso de los mismos al recinto policial y a sus dependencias Interiores.

a.3) Usos previstos: Control de la seguridad de los edificios policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios que presten sus servicios en el edificio, así como personal contratado, personal de limpieza, de mantenimiento, empresas colaboradoras, etc.

b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado, directamente en soporte papel o a través de vía telemática, o a partir de los datos existentes en el fichero SIGESPOL.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo documento nacional de identidad/número de identificación fiscal, nombre y apellidos, fecha y lugar de nacimiento, correo electrónico, despacho, situación administrativa, número de registro personal, fotografía, vehículos autorizados para la entrada en el recinto.

Datos de detalles de empleo: Cuerpo, escala, categoría, grado, puestos de trabajo o, en su caso, empresa de pertenencia.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Jefaturas de Unidades y dependencias de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía, que tengan instalada esta aplicación.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: ADDNIFIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ADDNIFIL.
a.2) Finalidad: Gestión del documento nacional de identidad.
a.3) Usos previstos: Identificación de los ciudadanos españoles.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Ciudadanos españoles solicitantes del documento nacional de identidad.
b.2) Procedencia y procedimiento de recogida: A partir de las solicitudes de expedición o renovación del documento nacional de identidad.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos de carácter identificativo: Datos de filiación (apellidos, nombre, fecha y lugar de nacimiento, sexo, nacionalidad, nombre de los padres).
– datos de características personales: Número del documento nacional de identidad, domicilio, teléfono, correo electrónico, fotografía, firma y huellas.
– datos incorporados electrónicamente en el chip: Datos de filiación del titular, imágenes digitalizadas de la fotografía y de la firma manuscrita, plantilla de impresión dactilar de los dedos índice o de los que proceda en su defecto y certificados reconocidos de autenticación y de firma, y claves públicas y privadas de los mismos.
– datos relativos a la expedición del documento: Número de soporte, equipo de expedición, datos del Registro Civil donde conste inscrito el nacimiento.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Fuerzas y Cuerpos de Seguridad, en virtud de lo establecido en la Ley Orgánica 2/1986, de 13 de marzo, así como en la Ley de Enjuiciamiento Criminal, para el cumplimiento de las funciones que tienen encomendadas como miembros de la Policía Judicial; a las Instituciones, órganos jurisdiccionales y Ministerio Fiscal, en virtud de lo establecido en el artículo 11.2 d) y e) de la Ley Orgánica 15/1999, de 13 de diciembre, así como cuando la cesión esté autorizada en una ley conforme a lo dispuesto en el artículo 11.2.a) de dicha Ley Orgánica.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: Unidad de Documentación de Españoles y Archivo, calle Julián González Segador, s/n, 28043 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Unidad de Documentación de Españoles y Archivo, calle Julián González Segador, s/n, 28043 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: ADEXTTRA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ADEXTTRA.

a.2) Finalidad: Gestión de trámites, informes y resoluciones seguidos en procedimientos de aplicación de la normativa relativa a la seguridad ciudadana y de la normativa de extranjería (visados en frontera y en el interior, denegaciones de entrada y regreso, y actividades de vigilancia e inspección en fronteras estancias y sus prórrogas, permisos de residencias y trabajo, renovaciones de autorizaciones, devoluciones, expulsiones, infracciones, sanciones, prohibiciones de entrada y cuantos otros se deriven de servicios de inspección, determinación de identidad y controles realizados en aplicación de la normativa de extranjería), de la normativa de comunitarios, de la normativa de apátrida, de la de asilo y de la protección subsidiaria, de trámites e informes de nacionalidad, y de menores extranjeros indocumentados o en situación legal de desamparo y la gestión de expedición de títulos de viaje o documento similar a asilados, apátridas e indocumentados.

a.3) Usos previstos: Actuaciones administrativas que no resulten necesarias para la represión de infracciones penales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Ciudadanos extranjeros, comunitarios o extracomunitarios que accedan o se hallen regular o irregularmente en España y de ciudadanos españoles cuyos actos estén afectados por la normativa sobre extranjería.

b.2) Procedencia y procedimiento de recogida: Grabación de datos a través de terminal a partir de formularios diversos cumplimentados por el ciudadano comunitario o extranjero o su representante; diligencias, trámites o actuaciones policiales o resoluciones de las Autoridades gubernativas o judiciales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

De mayores de edad: Filiación: Nombre, apellidos, fecha y lugar de nacimiento, nombre de los padres, sexo.

Personales: Nacionalidad, domicilio, teléfono, fax, e-mail, estado civil, profesión, fotografía, pasaporte, documento nacional de identidad, impresiones dactilares, imágenes, voz, firma, número de identidad de extranjero, datos de familiares a cargo o de los que dependa, empresa y actividad laboral, número de seguridad social, representante legal, propiedades y posesiones, alojamiento y vivienda, ingresos y rentas, convivencia y arraigo, conducta, antecedentes, y cualquier otro que pudiera ser identificativo de la persona.

De menores indocumentados o en situación legal de desamparo: Nombre y apellidos, fecha y lugar de nacimiento, sexo, nacionalidad, domicilio, centro de acogida o lugar de residencia, teléfono, última residencia en el país de procedencia, impresiones dactilares, fotografía, Organismo Público bajo cuya protección se halle, informe médico forense de resultado de la prueba ósea de determinación de la edad, marcas y deficiencias físicas y psíquicas, tatuajes, características físicas o antropométricas, situación de indocumentado o de situación legal de desamparo; nombre, apellidos y domicilio de los padres, tutores o guardadores y cualquier otro dato de relevancia a los citados efectos identificadores.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios:

De mayores de edad: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre; a los órganos de la Administración del Estado con competencia en materia de extranjería e inmigración (Ministerios de Presidencia, Trabajo e Inmigración, Exteriores y de Cooperación, Justicia), y cuantos otros se contemplan en la Ley Orgánica

4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, reformada por la Ley Orgánica 8/2000, de 22 de diciembre, la Ley Orgánica 11/2003, de 29 de septiembre, de medidas concretas en materia de seguridad ciudadana, violencia doméstica e integración social de los extranjeros, la Ley Orgánica 14/2003, de 20 de noviembre, de Reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, modificada por la Ley Orgánica 8/2000, de 22 de diciembre; de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local; de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y de la Ley 3/1991, de 10 de enero, de Competencia Desleal, así como por la Ley Orgánica 2/2009, de 11 de diciembre, y normas de desarrollo.

De menores: Exclusivamente a instituciones públicas nacionales encargadas de la protección de menores y aquéllos que prevé la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos:

De mayores de edad: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

De menores: Exclusivamente a instituciones públicas extranjeras encargadas de la protección de menores y aquéllos que prevé la Ley Orgánica 15/1999, de 13 de diciembre.

f) Órgano responsable del fichero: Comisaría General de Extranjería y Fronteras, calle General Pardiñas, 90, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Extranjería y Fronteras, calle General Pardiñas, 90, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: ADN-HUMANITAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ADN-HUMANITAS.

a.2) Finalidad: Identificación genética de personas desaparecidas, cadáveres y restos humanos sin identificar, de interés público, social y judicial, en investigaciones del Cuerpo Nacional de Policía.

a.3) Usos previstos: De acuerdo a la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, el uso previsto es para los procedimientos de identificación de restos cadavéricos o de averiguación de personas desparecidas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Restos humanos, personas desaparecidas y cadáveres sin identificar, así como aquellas personas genéticamente relacionadas con ellos, y las que determinen los Jueces y Tribunales en el uso de sus atribuciones.

b.2) Procedencia y procedimiento de recogida: Actividades de investigación e identificación de restos humanos realizadas por el Cuerpo Nacional de Policía, así como toma de las muestras referidas en el apartado anterior para los correspondientes cotejos identificativos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Perfiles genéticos, obtenidos de muestras biológicas, los cuales proporcionen, exclusivamente, información genética reveladora de la identidad de la persona, sexo, ancestralidad y rasgos físicos externos, sin que en ningún momento de dichos perfiles se extraiga información relativa a la salud de las personas.

Datos de carácter identificativo: descripción, rasgos fisonómicos, antropológicos y datos del perfil genético con valor identificativo.

Datos de características personales y de identidad: DNI/NIF/Pasaporte, nombre y apellidos, dirección postal, teléfono, datos filiación, datos familiares, fecha y lugar de nacimiento, edad, sexo, nacionalidad, lugares de estancia habitual.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Según lo establecido en la Ley Orgánica 10/2007, de 8 de octubre:

Los datos sólo podrán utilizarse por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas de la Policía y de la Guardia Civil en el ejercicio de sus funciones; así como por las Autoridades Judiciales y Fiscales; quienes en todos los casos, sólo los utilizarán en la investigación de los casos de identificación para los que fueron obtenidos.

Los datos podrán cederse a las Policías Autonómicas que sólo los utilizarán para la investigación de los casos de identificación de cadáveres o averiguación de personas desaparecidas, para los que fueron obtenidos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: De conformidad con lo establecido en la Ley Orgánica 10/2007, de 8 de octubre, podrán cederse los datos a las Autoridades Judiciales, Fiscales o Policiales de terceros países, de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes.

f) Órgano responsable del fichero: Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

5. FICHERO: ADN-VERITAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ADN-VERITAS.

a.2) Finalidad: Cooperar con la Administración de Justicia en el esclarecimiento de infracciones penales, con la identificación genética de vestigios biológicos recogidos en la investigación de hechos presuntamente delictivos o de muestras de la misma naturaleza, en investigaciones realizadas por el Cuerpo Nacional de Policía en el ámbito de sus competencias, de acuerdo con lo establecido en la Ley Orgánica 2/1986, de 13 de marzo.

a.3) Usos previstos: Para los procedimientos de averiguación e identificación en investigaciones de hechos presuntamente delictivos o criminales, de acuerdo con la Ley Orgánica 10/2007, de 8 de octubre, y de la Ley de Enjuiciamiento Criminal en lo relativo al Titulo V, del libro II, de la comprobación del delito y averiguación del delincuente.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas que determinen los Jueces y Tribunales, en el ejercicio de las funciones que tienen legalmente atribuidas, las relacionadas con restos humanos o vestigios que constituyan objeto de análisis, las relacionadas con hechos presuntamente delictivos investigados que voluntariamente se sometan al tratamiento y los sospechosos, detenidos o imputados, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el

patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados (artículo 3 de la Ley Orgánica 10/2007, de 8 de octubre) y según lo establecido en los artículos 326 y 363 de la Ley de Enjuiciamiento Criminal.

b.2) Procedencia y procedimiento de recogida: Actividades de investigación realizadas por el Cuerpo Nacional de Policía, en el cumplimiento de sus funciones de averiguación e identificación en investigaciones de hechos presuntamente delictivos o criminales, conforme a los procedimientos establecidos en la legislación vigente, recogidos del colectivo indicado, mediante formulario, transmisión electrónica de datos/Internet y diversos análisis de laboratorio ya sea en soporte papel, vía telemática o soporte informático o magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Perfiles genéticos, obtenidos de muestras biológicas, los cuales proporcionen, exclusivamente, información genética reveladora de la identidad de la persona, sexo, ancestralidad y rasgos físicos externos, sin que en ningún momento de dichos perfiles se extraiga información relativa a la salud de las personas.

Datos de carácter identificativo: descripción, rasgos fisonómicos, antropológicos y datos del perfil genético con valor identificativo.

Datos de características personales y de identidad: DNI/NIF/Pasaporte, nombre y apellidos, dirección postal, teléfono, datos filiación, datos familiares, fecha y lugar de nacimiento, edad, sexo, nacionalidad, lugares de estancia habitual.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios:

Los datos solo podrán utilizarse por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado, entendiendo por tales las Unidades respectivas de la Policía y de la Guardia Civil en el ejercicio de sus funciones; así como por las Autoridades Judiciales y Fiscales, en la investigación de los delitos enumerados en la Ley Orgánica 10/2007, de 8 de octubre, y en el marco de la averiguación de cualquier hecho delictivo conforme a lo estipulado en la Ley de Enjuiciamiento Criminal en lo relativo al Título V, del libro II, de la comprobación del delito y averiguación del delincuente.

Los datos podrán cederse a las Policías Autonómicas que sólo los utilizarán para la investigación de los delitos referidos en la citadas Leyes Orgánicas y al Centro Nacional de Inteligencia para la prevención de tales delitos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: De conformidad con lo establecido en la Ley Orgánica 10/2007, de 8 de octubre, podrán cederse los datos a las Autoridades Judiciales, Fiscales o Policiales de terceros países, de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes.

f) Órgano responsable del fichero: Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

6. FICHERO: ADPASFIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ADPASFIL.

a.2) Finalidad: Gestión de expedición de pasaportes a ciudadanos españoles y títulos de viaje o documento similar a asilados, apátridas e indocumentados.

a.3) Usos previstos: La identificación de los ciudadanos españoles que residan o se desplacen al extranjero.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Ciudadanos españoles solicitantes de pasaporte y ciudadanos extranjeros a los que se les expida por habérseles concedido el derecho de asilo, el estatuto de apátrida o documentación de indocumentado.

b.2) Procedencia y procedimiento de recogida: A partir de las solicitudes de pasaporte, título de viaje o documento similar.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Filiación: Apellidos, nombre, fecha y lugar de nacimiento, nombre de los padres, sexo.

Personales: Documento nacional de identidad, domicilio, teléfono, nacionalidad, NIE, fotografía, firma, huellas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Fuerzas y Cuerpos de Seguridad, en virtud de lo establecido en la Ley Orgánica 2/1986, de 13 de marzo, así como en la Ley de Enjuiciamiento Criminal, para el cumplimiento de las funciones que tienen encomendadas como miembros de la Policía Judicial; a las Instituciones, órganos jurisdiccionales y Ministerio Fiscal, en virtud de lo establecido en el artículo 11.2 d) y e) de la Ley Orgánica 15/1999, de 13 de diciembre, así como cuando la cesión esté autorizada en una ley conforme a lo dispuesto en el artículo 11.2.a) de dicha Ley Orgánica.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales), así como a las autoridades consulares a efectos del Real Decreto 896/2003, de 11 de julio, por el que se regula la expedición del pasaporte ordinario y se determinan sus características.

f) Órgano responsable del fichero: Unidad de Documentación de Españoles y Archivo, calle Julián González Segador, s/n, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Unidad de Documentación de Españoles y Archivo, calle Julián González Segador, s/n, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

7. FICHERO: ALUMNOS DEL CENTRO FORMACIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Alumnos del centro formación.

a.2) Finalidad: Realizar un seguimiento de los alumnos inscritos en los distintos cursos, tanto a nivel de identificación personal como de la evolución académica registrada durante todo el curso.

a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios del Cuerpo Nacional de Policía y aspirantes a ingresar en el Cuerpo, que cursan estudios o realizan prácticas dependientes del Centro de Formación.

b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado, en soporte papel y en soporte magnético de otros ficheros de la Dirección General, creados para la selección y gestión de recursos humanos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos, documento nacional de identidad, nombre y apellidos, dirección, teléfono, otros: Matrícula automóvil.

Datos personales: fecha de nacimiento.

Datos académicos y profesionales: Formación, titulaciones, historial de estudiante y experiencia profesional.

Datos de detalles de empleo: Cuerpo, escala, categoría, grado, historial del trabajador.

Datos relativos a comisión de infracciones: Infracciones administrativas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: División de Formación y Perfeccionamiento, avenida Pío XII, 50, 28016 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Formación y Perfeccionamiento, Avenida Pío XII, 50, 28016 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

8. FICHERO: Archivo SISS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Archivo SISS.

a.2) Finalidad: Gestión expedientes de investigación en fraudes a la Seguridad Social.

a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas, jurídicas implicadas en fraudes a la Seguridad Social.

b.2) Procedencia y procedimiento de recogida: Manual, a partir de los datos de las investigaciones.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y personales (documento nacional de identidad, número de identificación fiscal, nombre y apellidos y domicilio, teléfono, marcas físicas, modus operandi, vehículos, estado civil, fecha y lugar de nacimiento, sexo, nacionalidad). Infracciones penales y administrativas, datos de circunstancias sociales, académicos y profesionales, de detalles de empleo y carrera administrativa, de información comercial, económicos y financieros, y de transacciones.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados o convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28033 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

9. FICHERO: ARCHIVO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ARCHIVO.

a.2) Finalidad: Gestionar la información de los ficheros manuales de archivo de las dependencias policiales de la Dirección General de la Policía y de la Guardia Civil. Control de expedientes.

a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas incluidas en los asuntos tramitados en las dependencias policiales.

b.2) Procedencia y procedimiento de recogida: Los datos se graban por los gestores de la información a partir de los documentos, declaraciones y formularios, archivados en los ficheros manuales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos de carácter personal: Documento de identidad, nombre y apellidos, fecha y lugar de nacimiento, domicilio, nacionalidad, etc.

Datos del documento archivado: Número de expediente y legajo, asunto, etcétera.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Jefaturas de Unidades y dependencias de la Dirección General de la Policía y de la Guardia Civil que tengan instalada esta aplicación.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

10. FICHERO: ATRABAN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ATRABAN.
a.2) Finalidad: Elaboración de los boletines informativos y estadísticos sobre los atracos a entidades bancarias.
a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas implicadas en actividades delictivas de carácter penal.
b.2) Procedencia y procedimiento de recogida: Manual, a partir de la comunicación de los hechos delictivos cursada por las distintas plantillas policiales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y personales (documento nacional de identidad/número de identificación fiscal, nombre y apellidos y domicilio, fecha y lugar de nacimiento, sexo, nacionalidad, fotografías). Datos del hecho delictivo.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados o convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28033, Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

11. FICHERO: CADAPIP (Carpeta Dossier).

(Suprimido)

12. FICHERO: COMIROGA-IP.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: COMIROGA-IP.
a.2) Finalidad: Atención a los requerimientos de cooperación internacional necesarios para la ejecución de comisiones rogatorias.
a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas implicadas en actividades delictivas de carácter penal objeto de comisiones rogatorias.
b.2) Procedencia y procedimiento de recogida: Manual, a partir de la recepción oficial de la solicitud de colaboración.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y personales (documento nacional de identidad/número de identificación fiscal, nombre y apellidos y domicilio, fecha y lugar de nacimiento, sexo, nacionalidad). Infracciones penales y administrativas.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: División de Cooperación Internacional, calle Julián González Segador, sin número, 28043 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Cooperación Internacional, calle Julián González Segador, sin número, 28043 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

13. FICHERO: CONTROL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: CONTROL.
a.2) Finalidad: Gestionar información sobre inspecciones fronterizas, vigilancia de fronteras, actividades relevantes para la seguridad ciudadana y objetos de interés policial.
a.3) Usos previstos: Control policial de actividades relevantes para la seguridad ciudadana y de personas que entran y salen del territorio español.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas cuyo paso sea controlado en puestos fronterizos, o controladas como consecuencia del alquiler de vehículos, compraventa o pignoración de efectos, hospederías, visitas a centros o instalaciones oficiales, eventos especiales, y otros controles policiales de personas y objetos numerados.
b.2) Procedencia y procedimiento de recogida: Los datos se graban, vía teleproceso, por los gestores de la información, a partir de las actividades policiales de control de fronteras, establecimientos de compraventa o pignoración, alquiler de vehículos, partes de viajeros, dispositivos operativos, etc.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de identidad de la persona controlada policialmente: Documento nacional de identidad, nombre y apellidos, domicilio, nombre de los padres, fecha y lugar de nacimiento, sexo, teléfono, fotografía, nacionalidad, pasaporte, número de identidad de extranjero, impresiones dactilares, representante legal y cualquier otro que pudiera ser identificativo de la persona.

Datos identificadores del objeto: tipo, marca, modelo, numeración o matriculación, descripción, etc.

Datos identificadores del control: lugar, motivo, fecha, hora, duración, etcétera.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Extranjería y Fronteras, calle General Pardiñas, 90, 28071 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Extranjería y Fronteras, calle General Pardiñas, 90, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

14. FICHERO: DULCINEA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: DULCINEA.

a.2) Finalidad: Investigación y recogida de los datos necesarios, que afecten a la seguridad pública e infracciones penales, dentro del campo de competencia de la Brigada del Patrimonio Histórico.

a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas, jurídicas u organismos públicos y privados, cuya actividad guarde relación con la normativa que ampara la protección del Patrimonio Histórico.

b.2) Procedencia y procedimiento de recogida: Los datos proceden de Administraciones públicas, entidades privadas, propios interesados y otras fuentes propias de la investigación.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y personales documento nacional de identidad/número de identificación fiscal, nombre y apellidos y domicilio, teléfono, marcas físicas, modus operandi, vehículos, estado civil, fecha y lugar de nacimiento, sexo, nacionalidad. Infracciones penales y administrativas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios suscritos por España (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

15. FICHERO: EXPEDIENTES DEPORTIVOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Expedientes Deportivos.

a.2) Finalidad: Registro de actividades deportivas de los funcionarios tanto a nivel individual como formando equipo en competiciones deportivas.

a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios del Cuerpo Nacional de Policía, de otros cuerpos y fuerzas de seguridad, militares y equipos federados.

b.2) Procedencia y procedimiento de recogida: Aportación voluntaria de los propios interesados bien directamente o a través de los órganos de que dependan laboralmente o federación deportiva.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos, documento nacional de identidad, nombre y apellidos.
Datos personales: Categoría deportiva.
Datos de circunstancias sociales: pertenencia a Clubes, asociaciones, etcétera.
Datos de detalles de empleo: Cuerpo, escala, categoría, grado, puesto de trabajo.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Las que pudieran derivarse de la aplicación de los artículos 11 y 21 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: División de Formación y Perfeccionamiento, avenida Pío XII, 50, 28016 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Formación y Perfeccionamiento, avenida Pío XII, 50, 28016 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

16. FICHERO: EXTRADICIONES-IP.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Extradiciones-IP.
a.2) Finalidad: Atención a los requerimientos de cooperación internacional necesarios para la ejecución de extradiciones.
a.3) Usos previstos: Cumplimentación y control de extradiciones.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas incursas en procesos de extradición conforme a la normativa en vigor.
b.2) Procedencia y procedimiento de recogida: Manual, a partir de la recepción oficial de la solicitud de extradición.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y personales (documento nacional de identidad/número de identificación fiscal, nombre y apellidos y domicilio, fecha y lugar de nacimiento, sexo, nacionalidad). Infracciones penales.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: División de Cooperación Internacional, calle Julián González Segador, sin número, 28043 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Cooperación Internacional, calle Julián González Segador, sin número, 28043 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

17. FICHERO: GATI.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: GATI.
a.2) Finalidad: La prevención de peligros reales concretos para la seguridad pública y represión de infracciones penales mediante la recuperación, evaluación, tratamiento, coordinación y análisis de toda la información generada por las unidades operativas del Cuerpo Nacional de Policía, así como la creación de inteligencia criminal, de acuerdo a lo establecido en el artículo 22.4 de la Ley Orgánica 15/1999, de 13 de diciembre.
a.3) Usos previstos: Actuaciones de Fuerzas y Cuerpos de Seguridad con fines policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas detenidas e investigadas, o relacionadas con éstas, así como víctimas de infracciones penales, testigos y denunciantes de las mismas.

b.2) Procedencia y procedimiento de recogida: La información es facilitada por las unidades operativas y obtenida en el transcurso de su labor de investigación dirigida a la prevención de peligros reales para la seguridad pública y represión de infracciones penales, así como la facilitada por otros países u organismos internacionales en virtud de los acuerdos y tratados de cooperación policial.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Documento nacional de identidad/número de identificación fiscal, número de la Seguridad Social/Mutualidad, nombre y apellidos, domicilios y características de éstos, teléfono, firma, huella digitalizada, fotografía, voz, marcas físicas, estado civil, filiación, fecha y lugar de nacimiento, sexo, nacionalidad, lengua materna, características físicas y antropométricas, peligrosidad, propiedades, posesiones, licencias, permisos, vehículos, pertenencia a organizaciones criminales, datos laborales, categoría, grado, puestos de trabajo, historial, actividades y negocios, inversiones, datos bancarios y tarjetas crédito y en los casos que les fuera indispensable, aquellos datos a que se refieren los apartados 2 y 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

18. FICHERO: GESACCES.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: GESACCES.

a.2) Finalidad: Gestionar la identificación y autenticación, así como el control de todos los accesos a las aplicaciones informáticas de la Dirección General de la Policía, residenciadas en el Centro de Proceso de Datos de El Escorial.

a.3) Usos previstos: Auditoría e inspección sobre el uso de los datos informatizados. Se prevé el control de todos los ficheros policiales y, en su caso, investigación de aquellos usos contrarios a la deontología profesional y constitutivos de infracción.

b) Origen de los datos:

b.1) Colectivo: Todos los usuarios autorizados a acceder a las aplicaciones informáticas residenciadas en el Área de Informática de la Dirección General de la Policía.

b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado, directamente en soporte papel o a través de vía telemática. Los datos de los accesos se graban automáticamente.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de identificación del usuario: Documento nacional de identidad, nombre, apellidos, clave y contraseña de acceso a las aplicaciones, plantilla de destino, cuerpo al que pertenece y número del carné profesional, fecha cambio clave, fecha de autorización, fecha de baja, datos certificado DNI, organismo de pertenencia del funcionario.

Datos de conexión (fecha y hora de conexión y desconexión de la aplicación, tipo de acceso, registro accedido, etc.) necesarios para hacer un control efectivo de seguridad.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: No se prevén.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Subdirección General de Logística, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Subdirección General de Logística, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

19. FICHERO: GESTIÓN LIBROS, LECTORES, PRÉSTAMOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión libros, lectores, préstamos.

a.2) Finalidad: Control de la gestión de la biblioteca, tanto a nivel de los fondos documentales, como a la gestión de préstamos y lectores.

a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios destinados en la Dirección General de la Policía y otros organismos públicos.

b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado directamente en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos, documento nacional de identidad, nombre y apellidos, dirección, teléfono.

Datos de detalles de empleo: Cuerpo, escala, categoría, grado, puesto de trabajo.

Datos transacciones: Bienes y servicios recibidos por el afectado.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: División de Formación y Perfeccionamiento, Avenida Pío XII, 50, 28016 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Formación y Perfeccionamiento, Avenida Pío XII, 50, 28016 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

20. FICHERO: GESTIÓN DE OPOSICIONES Y ACREDITACIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión de oposiciones y acreditaciones.
a.2) Finalidad: Gestionar las oposiciones y procesos selectivos de ingreso y promoción del Cuerpo Nacional de Policía y las pruebas de acreditación de Vigilantes de Seguridad y sus especialidades, así como acreditar a los profesores para impartir docencia en Centros de Formación de Vigilantes.
a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Cualquier persona que solicite participar en oposiciones o procesos de promoción interna en el Cuerpo Nacional de Policía y pruebas de selección para Vigilantes de Seguridad y sus especialidades o acreditarse como profesor de vigilantes.
b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado directamente en soporte papel o mediante grabación de los datos en el caso de instancias presentadas a través de la sede electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos, documento nacional de identidad, nombre y apellidos, dirección, teléfono.
Datos personales: Fecha y lugar de nacimiento, nombre de los padres, edad y sexo.
Datos académicos y profesionales: Titulaciones académicas, trayectoria profesional y resultado de las pruebas.
Datos de detalles de empleo: Cuerpo, escala, categoría, situación laboral y puesto de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Las que pudieran derivarse de la aplicación de los artículos 11 y 21 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: División de Formación y Perfeccionamiento, Avenida Pío XII, 50, 28016 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Formación y Perfeccionamiento, Avenida Pío XII, 50, 28016 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

21. FICHERO: GRUME.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: GRUME.
a.2) Finalidad: Gestión de la información correspondiente a menores de edad de interés policial.
a.3) Usos previstos: Investigaciones policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Menores de edad de interés policial y personas relacionadas con ellos.
b.2) Procedencia y procedimiento de recogida: La información es grabada por los gestores a partir de las reseñas inspecciones oculares o asuntos investigados por la Dirección General de la Policía y de la Guardia Civil.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre, apellidos, dirección, teléfono, marcas físicas, datos de familia, lugar y fecha de nacimiento, características físicas y antropométricas, alojamiento y vivienda.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

22. FICHERO: INSPECCIONES Y CONTROL DEL JUEGO.

(Suprimido)

23. FICHERO: LOCUPOL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: LOCUPOL.
a.2) Finalidad: Investigaciones encaminadas a la actualización y establecimiento de las referencias y sistemas de análisis en las que se sustentan las bases científicas de los informes periciales emitidos por el Laboratorio de Acústica Forense y otro tipo de investigaciones científico-forenses relacionadas con la acústica y las ciencias del habla.
a.3) Usos previstos: Investigaciones policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que voluntariamente o por orden judicial, presten su voz, siempre que las características de tal emisión se adecuen a los objetivos y procedimientos de análisis relacionados con las investigaciones correspondientes.
b.2) Procedencia y procedimiento de recogida: Cumplimentar una ficha de datos personales y grabación microfónica y telefónica de una muestra de voz.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: voz y datos de filiación de informantes; residencia de los progenitores, nivel de formación académica, patologías, traumatismos o problemas físicos relacionados con el aparato respiratorio y fonador; hábitos en relación con el tabaco y complexión física.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Científica, Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

24. FICHERO: OBJETOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: OBJETOS.

a.2) Finalidad: Gestionar información de órdenes de búsqueda de objetos (vehículos, ciclomotores, maquinaria en general, armas, documentos de identidad, billetes de banco, recetas médicas, joyas, obras de arte, electrodomésticos, etc.), motivadas por denuncias por robo, apropiación indebida, implicación en hechos delictivos, etc.

a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Propietario del objeto y/o denunciante de los hechos.

b.2) Procedencia y procedimiento de recogida: Los datos se graban, vía teleproceso, por los gestores de la información, a partir de las denuncias o de las órdenes de búsqueda cursadas por las autoridades judiciales, policiales o administrativas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales de carácter identificativo del propietario del objeto ylo del denunciante (nombre, apellidos, domicilio, teléfono).

Datos identificadores del objeto (marca, modelo, color, tipo, número, número de motor, número de bastidor, matricula, y cualquier otro dato susceptible de identificar al objeto) o relacionados con el mismo (valoración).

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los

artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

25. FICHERO: PERPOL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: PERPOL.

a.2) Finalidad: Gestión de antecedentes de las personas de interés policial, con sujeción a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, y especialmente en su artículo 22.4: órdenes de búsqueda, reseñas, hechos que se les imputan y resoluciones judiciales.

a.3) Usos previstos: Investigación policial y comprobación de la existencia de requisitorias judiciales o policiales.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas nacionales y extranjeras que tengan órdenes de búsqueda vigentes o cesadas, que hayan sido detenidas o se haya demostrado su implicación en hechos delictivos o sobre las que haya recaído alguna resolución judicial; también los conceptuados policialmente como delincuentes activos y cadáveres sin identificar.

b.2) Procedencia y procedimiento de recogida: Los datos se graban, vía teleproceso, por los gestores de la información, a partir de las requisitorias cursadas por las autoridades judiciales, policiales o administrativas, de las reseñas llevadas a cabo por los gabinetes de Policía Científica, de los atestados policiales instruidos por la Brigadas y Grupos Operativos, y de las resoluciones dictadas por las autoridades judiciales o administrativas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Documento de identidad, nombre y apellidos, domicilios, fórmulas e imágenes lofoscópicas, estado civil, nombre de los padres, fecha y lugar de nacimiento, nacionalidad, descripción y marcas físicas, sexo, imagen, voz, fotografía y cualquier otro dato que pudiera ser identificativo de la persona. Conceptuación policial, peligrosidad, trabajo, órdenes de búsqueda, reseñas, hechos imputados y resoluciones judiciales y administrativas. El descriptor ADN, para los cadáveres sin identificar y grupo de riesgo de personas desaparecidas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

Los datos relativos a menores podrán ser objeto de trasferencia al National Center for Missing eExploited Childrán de Estados Unidos (Centro Nacional para Menores Desaparecidos y Explotados) con el consentimiento expreso de sus representantes legales.

f) Órgano responsable del fichero: Unidad de Documentación de Españoles y Archivo, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Unidad de Documentación de Españoles y Archivo, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

26. FICHERO: RECLAMACIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: RECLAMACIÓN.

a.2) Finalidad: Gestión de las reclamaciones administrativas de contenido económico realizadas por funcionarios de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía.

b.2) Procedencia y procedimiento de recogida: A partir de los datos existentes en el fichero SIGESPOL.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Número de documento nacional de identidad, nombre y apellidos, categoría profesional, destino.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: División de Coordinación Económica y Técnica, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Coordinación Económica y Técnica, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

27. FICHERO: REGISTRO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: REGISTRO.

a.2) Finalidad: Gestionar la información de los documentos tramitados en las dependencias policiales de la Dirección General de la Policía Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía, en lo referente al registro de entrada y salida de correspondencia oficial, fax, etc.
a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas incluidas en los documentos tramitados.
b.2) Procedencia y procedimiento de recogida: Los datos se graban por los gestores de la información a partir de los documentos recepcionados o remitidos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos de carácter personal: documento de identidad, nombre y apellidos, fecha y lugar de nacimiento, domicilio, nacionalidad, etc.
Datos del documento tramitado: número de registro y fecha de entrada o salida, asunto, origen, destino y referencia al contenido del documento.

c.2) Sistema de tratamiento: Parcialmente Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Órgano o unidad administrativa destinatario de la documentación, conforme a lo establecido por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Jefaturas de Unidades y Dependencias de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía, que tengan instalada esta aplicación.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

28. FICHERO: S.A.I.D.

(Suprimido)

29. FICHERO: SEGURPRI.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SEGURPRI.
a.2) Finalidad: Gestión y control de seguridad privada de empresas, departamentos de seguridad, vigilantes de seguridad, vigilantes de explosivos, escoltas privados, jefes y directores de seguridad, detectives privados, procedimientos sancionadores en materia de seguridad privada y contratos de servicios.
a.3) Usos previstos: Gestión del control en materia de seguridad privada.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Empresas, titulares, directivos y empleados de las mismas, vigilantes de seguridad privada, vigilantes de explosivos, escoltas privados, jefes y directores de seguridad y detectives privados.

b.2) Procedencia y procedimiento de recogida: Grabación de los datos procedentes del propio interesado, persona física o jurídica, o de su representante legal, y/o de otros órganos de la Dirección General de la Policía y/o Administraciones públicas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Documento nacional de identidad, apellidos y nombre, fecha de nacimiento y domicilio del personal de seguridad privada, así como datos de carácter social referidos a empleo, licencias, autorizaciones, situaciones laborales, sanciones y contratos, tanto de empresas como de empleados o clientes.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Comisaría General de Seguridad Ciudadana, calle Francos Rodríguez, 110, 28039 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Seguridad Ciudadana, calle Francos Rodríguez, 110, 28039 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

30. FICHERO: SIDENPOL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SIDENPOL.

a.2) Finalidad: Gestión de trámites necesarios que llevan las denuncias en las dependencias policiales.

a.3) Usos previstos: Tramitación informatizada de las denuncias e investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas incluidas en el atestado policial.

b.2) Procedencia y procedimiento de recogida: La información es grabada por los gestores a partir de las denuncias tramitadas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de identidad del denunciante, denunciado y personas incursas (documento de identidad, nombre y apellidos, domicilio, nombre de los padres, fecha y lugar de nacimiento, sexo, etc.).

Datos del hecho denunciado (descripción del hecho, lugar y fecha de comisión, circunstancias concurrentes, objetos sustraídos o afectados, etc.).

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección Adjunta Operativa, calle Rafael Calvo, 33, Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Unidad de Seguimiento y Control Operativo de la Dirección Adjunta Operativa, calle Rafael Calvo, 33, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

31. FICHERO: SIGESDOC-PC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SIGESDOC-PC.

a.2) Finalidad: Gestión de archivos y documentos de los asuntos investigados por los Servicios Centrales de la Comisaría General de Policía Científica.

a.3) Usos previstos: Gestión e investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas, jurídicas u organismos públicos y privados, objeto o relacionados con las actividades de la Comisaría General de Policía Científica.

b.2) Procedencia y procedimiento de recogida: Los datos proceden de los asuntos investigados por las Unidades de la Comisaría General de Policía Científica, de otras unidades policiales, de otras Administraciones Públicas, entidades privadas, propios interesados e intercambio de información.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos y personales (documento nacional de identidad/número de identificación fiscal, nombre y apellidos y domicilio, teléfono, firma/huella, imagen/voz, marcas físicas, modus operandi, vehículos, estado civil, fecha y lugar de nacimiento, sexo, nacionalidad). Infracciones penales y administrativas.

Datos del documento: número de expediente, asunto, fecha, etc.

c.2) Sistema de tratamiento: Parcialmente Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea

parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

32. FICHERO: SIGESDOC-PJ.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SIGESDOC-PJ.

a.2) Finalidad: Registro de entrada/salida/telefonemas y gestión de archivos y documentos de la Comisaría General de Policía Judicial.

a.3) Usos previstos: Gestión e investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas, jurídicas u organismos públicos y privados, cuya actividad guarde relación con las competencias propias de la Comisaría General.

b.2) Procedencia y procedimiento de recogida: Los datos proceden de Administraciones públicas, entidades privadas, propios interesados y otras fuentes de investigación e intercambio de información.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos y personales (documento nacional de identidad/número de identificación fiscal, nombre y apellidos y domicilio, teléfono, firma/huella, imagen/voz, marcas físicas, modus operandi, vehículos, estado civil, fecha y lugar de nacimiento, sexo, nacionalidad). Infracciones penales y administrativas, datos de circunstancias sociales, académicos y profesionales, de detalles de empleo y carrera administrativa, de información comercial, económicos y financieros, y de transacciones.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Judicial, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

33. FICHERO: SIGESPOL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SIGESPOL.

a.2) Finalidad: Gestión de asuntos relativos a los recursos humanos de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía, incluidos los relacionados con planes de pensiones, y a las condecoraciones policiales. Gestión de indemnizaciones por razón de servicio; trayectoria académica y docente de alumnos y profesores del Centro de Promoción; gestión de suscripciones, colaboraciones, envíos y cobros de las revistas policiales; y gestión de las prendas de uniformidad del personal.

a.3) Usos previstos: Administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Totalidad de recursos humanos afectos a la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía, personas ajenas a las que se les concede el ingreso en la Orden al Mérito Policial y beneficiarios de éstos.

b.2) Procedencia y procedimiento de recogida: Aportación voluntaria y obtención de oficio de otros organismos y unidades de otras Administraciones públicas, cuya cesión deba realizarse de acuerdo con la Ley.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: nombre y apellidos, documento nacional de identidad, lugar y fecha de nacimiento, sexo, estado civil, domicilio, número de registro personal, número de afiliación a la Seguridad Social y mutualidades, imagen (foto), certificados electrónicos y cuenta corriente.

Datos profesionales: Remuneraciones económicas, plantillas, destinos, categorías, felicitaciones y recompensas, puestos de trabajo, categoría, trienios, cursos, titulaciones y diplomas, sanciones disciplinarias y penales, armas que posean y licencias, distintivos, ayudas, carné de conducir, historial académico, suscripciones y colaboraciones a revistas policiales y talla antropométrica para uniformes.

Datos especialmente protegidos: Afiliación sindical, sanitarios, absentismo laboral.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios:

Al Registro Central de Personal en cumplimiento de lo establecido en el artículo 13 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública.

A la Agencia Estatal de la Administración Tributaria, en virtud de la Ley 40/1998, de 9 de diciembre.

A la Tesorería General de la Seguridad Social, en virtud del Real Decreto Legislativo 1/1994, de 20 de junio.

A la Mutualidad General de los Funcionarios Civiles del Estado, en virtud de la Ley 29/1975, de 27 de julio.

A la Dirección General de Costes de Personal y Pensiones Públicas, en virtud del Real Decreto Legislativo 670/1987, de 30 de abril, y previa petición de los funcionarios a entidades financieras para el abono de haberes, sindicatos, mutualidades, colegios de huérfanos y otras entidades para el abono de las cuotas.

A las entidades gestora y depositaria y a la Comisión de Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 19 de la Ley 61/2003, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2004, y el texto refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por el Real Decreto Legislativo 1/2002, de 29 de noviembre.

A la Intervención General de la Administración del Estado, al Tribunal de Cuentas y a las entidades financieras en que se realice el pago de haberes.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: División de Personal, Avenida Pío XII, 50, Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Personal, Avenida Pío XII, 50, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

34. FICHERO: TRASLADO DE CONDENADOS-IP.

a.1) Identificación del fichero: Traslado de condenados-IP.

a.2) Finalidad: Atención a los requerimientos de cooperación internacional necesarios para la ejecución de traslados de condenados.

a.3) Usos previstos: Colaboración judicial y policial de carácter internacional.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas en situación de cumplimiento efectivo de penas ingresadas en centros penitenciarios.

b.2) Procedencia y procedimiento de recogida: Manual, a partir de la recepción oficial de la solicitud del acuerdo de traslado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Manual, a partir de la recepción oficial de la solicitud del acuerdo de traslado.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: División de Cooperación Internacional, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la División de Cooperación Internacional, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

35 FICHERO: VISITAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: VISITAS.

a.2) Finalidad: Gestionar la información de las personas que acceden, con carácter excepcional, a dependencias e instalaciones policiales.

a.3) Usos previstos: Seguridad y control interno.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas ajenas a la propia plantilla que acceden o visitan dependencias policiales.

b.2) Procedencia y procedimiento de recogida: Los datos se graban por los gestores de la información a partir de la información facilitada por las personas cuyo acceso se autoriza.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos de carácter personal: documento de identidad, nombre y apellidos, domicilio, empresa o departamento al que representan, etc.

Datos de la visita: fecha y hora de la misma, motivo de la visita, departamento visitado, etc.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Jefaturas de Unidades y dependencias de la Dirección General de la Policía y de la Guardia Civil, ámbito del Cuerpo Nacional de Policía, que tengan instalada esta aplicación.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

36. FICHERO: BINCIPOL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: BINCIPOL.

a.2) Finalidad: Informatización de la tramitación y gestión de las investigaciones operativas, asignando un número único de asunto, así como un registro automático de entrada y salida de todos los documentos e informes que tengan entrada en Policía Científica. Seguimiento y control de los efectos y muestras que gestiona Policía Científica, mediante su identificación con etiquetas con código de barras, en aras de garantizar la cadena de custodia. Posibilidad de generar de forma automática todos los documentos propios del trabajo de Policía Científica, como son las actas de Inspección Ocular, Informes Periciales, y otros. Garantizar que quedan guardados en un formato no modificable mediante su firma digital.

Informatización de los trámites y gestiones que se realizan en Secretaría General como Asuntos Generales, así como del trámite de la reseña de detenidos, con las oportunas conexiones y transmisión de datos, entre otros, con los sistemas Perpol, Said y Lims.

Explotación de datos mediante el correspondiente sistema de consultas, así como mediante las relaciones operativas y de inteligencia, tanto de asuntos entre sí, como de muestras y efectos y resto de elementos integrados en los asuntos y generación automática de la estadística.

a.3) Usos previstos: Investigaciones realizadas por el Cuerpo Nacional de Policía con los citados fines.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Información relativa a personas, cadáveres y restos humanos que sean susceptibles de identificación en el ámbito de competencias de la policía científica.

b.2) Procedencia y procedimiento de recogida: Actividades de investigación e identificación de personas, cadáveres y restos humanos realizadas por el Cuerpo Nacional de Policía, así como toma de las muestras necesarias a tal fin para los correspondientes cotejos identificativos. Los datos recogidos serán introducidos en el sistema BINCIPOL por especialistas en policía científica de las respectivas unidades centrales y periféricas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Grado de implicación de personas en asuntos presuntamente delictivos.

Documento Nacional de Identidad/pasaporte/tarjeta única de extranjero.

Nombre y apellidos, nacionalidad, país de nacimiento, datos de filiación y sexo, fecha y lugar de nacimiento, nombre de los padres, domicilio, teléfonos y lugares de estancia habitual.

Vehículos utilizados y/o implicados en asuntos con identificación de propietario y/o conductor.

Descripción de rasgos fisonómicos y antropológicos.

Datos de reseña fotográfica, biográfica y biométrica con valor identificativo.

Ficheros electrónicos de voz, firma y escritura manuscrita, huellas e imágenes lofoscópicas y de fotografía facial.

Etiquetas descriptivas de elementos de voz, firma y escritura manuscrita, y vestigios lofoscópicos y de rasgos faciales para búsqueda de inteligencia científica.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Policía Científica, calle Julián González Segador, sin número, 28043 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

37. FICHERO: ARCHIVO DOCUMENTAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Archivo documental.

a.2) Finalidad: Albergar los documentos de cada órgano o unidad de la Dirección General de la Policía y de la Guardia Civil, en el ámbito del Cuerpo del Cuerpo Nacional de Policía, que se generan en el ejercicio de las funciones y competencias encomendadas al mencionado Cuerpo por la Ley Orgánica 2/1986, de 13 de marzo.

a.3) Usos previstos: Los policiales que se deriven del ejercicio de las competencias a que se refiere el epígrafe anterior.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todas aquellas personas que sean objeto del ejercicio de las competencias atribuidas al Cuerpo Nacional de Policía por la Ley Orgánica 2/1986, de 13 de marzo, bien como denunciantes, denunciados, detenidos, testigos, peritos, solicitantes o personas que sean objeto de las actividades policiales propias de los servicios públicos gestionados por la Dirección General de la Policía y de la Guardia Civil y funcionarios policiales intervinientes en las actuaciones.

b.2) Procedencia y procedimiento de recogida: Los datos serán recogidos en los documentos que deban elaborarse en el ejercicio de las competencias policiales que cada órgano o unidad deba desarrollar en cumplimiento de sus funciones.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Los documentos que contienen los datos se guardan cronológicamente ordenados en expedientes, que a su vez se almacenan en legajos sucesivos. Para su localización se utilizan fichas de cartón, en las que se recoge el nombre y apellidos de cada persona a que hacen referencia los documentos, el número de expediente y legajo en el que se hallan. Estas fichas se ordenan alfabéticamente por apellidos y nombre. Los datos personales contenidos en los documentos son todos aquellos que exija el procedimiento policial o administrativo que en cada caso se haya tramitado de acuerdo con las competencias ejercidas. Los datos que recogen los documentos, son todos aquellos que sean necesarios, en cada caso, para el desarrollo de las funciones encomendadas por la Ley al Cuerpo Nacional de Policía. Entre tales datos, a titulo orientativo, se enumeran los siguientes: Nombres, apellidos, número de documento nacional de identidad y de todo tipo de documentos, domicilios, fórmulas e imágenes lofoscópicas, estado civil, nombre de los padres, fechas y lugares de nacimiento, nacionalidad, descripción y marcas físicas, sexo, imagen, voz y cualquier otro que pudiera ser identificativo de la persona, peligrosidad, trabajo, órdenes de busca y captura, requisitorias en general, reseñas, hechos imputados y denunciados, resoluciones judiciales y administrativo policiales, bienes relacionados con hechos delictivos, etc.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los órganos jurisdiccionales y al Ministerio Fiscal, de conformidad con lo dispuesto en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo de Nacional de Policía).

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Ante los responsables de los respectivos órganos o unidades de la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía) de los que dependa cada archivo documental.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

38. FICHERO: ARPC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ARPC.
a.2) Finalidad: El registro de las actividades que comporta el desarrollo del Programa de Participación Ciudadana en el ámbito de la seguridad pública y de los participantes en el mismo.
a.3) Usos previstos: Gestión del Programa de Participación Ciudadana.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:
b.1) Colectivo: De colectivos ciudadanos y representantes de los mismos, que acuden a reuniones y actividades con representantes policiales en el ámbito del Programa de Participación Ciudadana.
b.2) Procedencia y procedimiento de recogida: Previo consentimiento expreso y por escrito de las personas físicas o jurídicas, en este caso a través de sus representantes legales, los datos son recogidos por los respectivos representantes policiales del programa y gravados en el programa, vía teleproceso.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo:
Del colectivo: Denominación, domicilio social, teléfono, fax.
De los representantes: nombre y representación que ostenta. Y reuniones o actividades en que participan.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039, Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

39. FICHERO: OND.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: OND.
a.2) Finalidad: Gestión de los expedientes sancionadores que se instruyen por infracciones tipificadas en la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.
a.3) Usos previstos: Gestión de las obligaciones derivadas de la Ley 19/2007, de 11 de julio, y del Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas y entidades organizadoras de competiciones y espectáculos deportivos y personas en general a las que se imputen infracciones tipificadas en el Título II de la Ley 19/2007, de 11 de julio.

b.2) Procedencia y procedimiento de recogida: La grabación se realizará a partir de los datos recogidos y enviados por los Coordinadores de Seguridad en el ejercicio de las funciones que les encomienda la Ley 19/2007, de 11 de julio, así como de aquellos otros que sean cedidos desde el Registro Central de Sanciones, de conformidad con la legislación vigente.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre y domicilio social de las entidades organizadoras de competiciones y espectáculos deportivos y de sus representantes legales, así como aquellos datos de identidad (DNI, nombre, apellidos, edad, lugar de nacimiento y domicilio) de las personas en general a las que se imputen las infracciones. Igualmente se recogerán los datos referentes al tipo de infracción imputada, trámites seguidos en el expediente y fecha de éstos, estado del mismo, propuesta de resolución formulada, resolución recaída y posibles sanciones impuestas con anterioridad no canceladas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los Órganos e Instituciones que se señalan en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre, a la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte, según lo previsto en la Ley 19/2007, de 11 de julio, a los Órganos competentes para imponer las sanciones que se recogen en el artículo 28 de la Ley 19/2007, de 11 de julio.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte.

f) Órgano responsable del fichero: Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

40. FICHERO: DGED-UCO

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: DGED-UCO

a.2) Finalidad: Registro de imágenes obtenidas de las grabaciones efectuadas en cumplimiento de lo establecido en los artículos 8, 12 y 14 de la Ley 19/2007, de 11 de julio, Contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

a.3) Usos previstos: Investigación policial de las infracciones penales y administrativas de las conductas descritas en los apartados 1 y 2 del artículo 2 de la Ley 19/2007, de 11 de julio.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que se encuentren en los recintos deportivos, o sus aledaños, en que se instalen elementos de captación de imágenes de conformidad con las previsiones de la Ley 19/2007, de 11 de julio.

b.2) Procedencia y procedimiento de recogida: Las imágenes son captadas por las cámaras de seguridad instaladas en los estadios deportivos. Desde éstas, se envían a la Unidad de Coordinación Operativa (UCO) correspondiente, con que deberá contar el respectivo recinto deportivo, dotada con los medios técnicos necesarios para su grabación. La UCO se encontrará bajo la dirección y supervisión del funcionario del Cuerpo Nacional de Policía, designado Coordinador de Seguridad al efecto.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Al margen de que en principio puedan recogerse la totalidad de las imágenes obtenidas a través de los sistemas de video vigilancia captadas por las cámaras de seguridad instaladas en los estadios deportivos, únicamente se guardarán las imágenes de personas y/o de colectivos presentes en aquellos incidentes que se hubieran podido producir como consecuencia o con ocasión de la celebración de un espectáculo deportivo, en el ámbito de captación de las cámaras, sobre las que se inicie algún procedimiento sancionador penal o administrativo, así como del lugar en que se han obtenido, y en su caso, los datos referentes a la identidad de las personas o colectivos a quienes correspondan las imágenes (Nombre, apellidos, edad, Documento Nacional de Identidad, domicilio, etc.), que hubieran sido obtenidos por la actuación de los miembros de las Fuerzas y Cuerpos de Seguridad en sus tareas de mantenimiento de la seguridad ciudadana.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras fuerzas y Cuerpos de Seguridad según lo previsto en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, a los Órganos e Instituciones que se señalan en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre, a la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte en los supuestos previstos en el artículo 28.1 de la Ley 19/2007, de 11 de julio, a los Órganos competentes para imponer las sanciones que se señalan en el artículo 28 de la Ley 19/2007, de 11 de julio.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte.

f) Órgano responsable del fichero: Comisaría General de Seguridad Ciudadana, C/ Francos Rodríguez, 104, 28039 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de la Comisaría General de Seguridad Ciudadana, c/ Francos Rodríguez, 104, 28039 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Dirección General de la Guardia Civil.

1. FICHERO: ACUARTELAMIENTOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Acuartelamientos.

a.2) Finalidad: Gestión y control de aspectos no económicos de los inmuebles y de los pabellones de la Guardia Civil.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titular del derecho de adjudicación a quien le ha sido cedido en uso alguno de los pabellones de la Guardia Civil. Personas físicas o jurídicas que oferten o mantengan contratos administrativos o privados con la Dirección General de Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Del propio interesado y de los contratos administrativos o privados, en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono y correo electrónico.
Datos de detalle de empleo: Cuerpo/Escala, Categoría/Grado, Puesto de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Guardia Civil - Jefatura de los Servicios de Apoyo, calle Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: ARMAMENTO Y EQUIPAMIENTO POLICIAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Armamento y equipamiento policial.
a.2) Finalidad: Control y gestión de armamento y material de equipamiento policial del personal de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal perteneciente a la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Del ingreso en academias y cambios de destino, según consta en las publicaciones y adjudicaciones de los jefes de las unidades, mediante soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.
Datos de detalle de empleo.

2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de los Servicios de Apoyo, c/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

3. FICHERO: ASISTENCIA LETRADA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Asistencia letrada.

a.2) Finalidad: Gestión y control de solicitudes de asistencia letrada al personal que presta sus servicios en la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) por el desempeño de sus funciones.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal implicado en procedimientos judiciales para los que se ha solicitado asistencia letrada.

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante la cumplimentación de los impresos de solicitud y de los datos de los informes emitidos a lo largo del procedimiento.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales o administratvivas: Infracciones penales.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.

Datos de detalle de empleo.

Otros tipos de datos: Situación procesal.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la Abogacía del Estado-Dirección del Servicio Jurídico del Estado (Ministerio de Justicia), de conformidad con lo dispuesto de la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica al Estado e Instituciones Públicas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Subdirección General de Personal, c/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

4. FICHERO: AUDITOR.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Auditor.
a.2) Finalidad: Gestionar la identificación y autenticación, así como el control de accesos a las aplicaciones y servicios de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil), así como auditar las transacciones realizadas.
a.3) Usos previstos: Investigación policial, auditoría y control de los usuarios que acceden a los sistemas y de los registros accedidos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todos los usuarios con capacidad para acceder a las aplicaciones informáticas de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).
b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado, directamente en soporte papel o a través de vía telemática.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, código de usuario, tarjeta de identidad profesional (TIP).
Datos de conexión.
Datos de la transacción realizada.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Servicios Técnicos, c/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

5. FICHERO: AYUDAS DE ESTUDIO.

(Suprimido)

6. FICHERO: BASE DE ASESORÍA JURÍDICA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Base de asesoría jurídica.
a.2) Finalidad: Elaboración de informes, tramitación de expedientes disciplinarios y administrativos y estudio de precedentes.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: El personal adscrito a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) y otro personal que se relacione con la misma dentro de su tráfico jurídico.

b.2) Procedencia y procedimiento de recogida: De las personas físicas o jurídicas que intervienen en los expedientes, a través de sus manifestaciones o actuaciones en cualquier tipo de soporte o medio.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.

Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales y administrativas.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.

Datos de características personales.

Datos de circunstancias sociales.

Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los Órganos Jurisdiccionales y al Ministerio Fiscal, según lo previsto en la Ley Orgánica 2/1989, de 13 de abril, Procesal Militar y de conformidad con el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de enero; al Ministerio de Defensa y al Ministerio del Interior, según lo previsto en la Ley Orgánica 2/1986, de 13 de marzo, Ley Orgánica 12/2007, de 22 de octubre, del Régimen Disciplinario de la Guardia Civil y y Ley 42/1999, del 25 de noviembre, de Régimen del Personal del Cuerpo de la Guardia Civil.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Asesoría Jurídica, c/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

7. FICHERO: COMPETICIONES DEPORTIVAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Competiciones deportivas.

a.2) Finalidad: Control de actividades deportivas del personal de las Fuerzas Armadas y Guardia Civil, tanto a nivel individual como formando equipo en competiciones deportivas, así como la gestión de los deportistas de élite de la Guardia Civil.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal del Cuerpo de la Guardia Civil y de las Fuerzas Armadas que participe en campeonatos o competiciones deportivas, y aquellos componentes de la Guardia Civil que soliciten la condición de deportista de élite de la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante formularios o correo electrónico en soporte papel o vía telemática.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono e imagen/voz.
Datos de características personales.
Datos de circunstancias sociales.
Datos académicos, profesionales y seguros.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Consejo Superior de Deportes de las Fuerzas Armadas y a las Juntas Centrales de Educación Física y Deportes de las Fuerzas Armadas, pevio consentimiento de los interesados.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Enseñanza, c/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

8. FICHERO: EMBARCACIONES.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Embarques.
a.2) Finalidad: Ejercicio de la función de Resguardo Fiscal del Estado y de la vigilancia y custodia de las costas, fronteras, espacio marítimo de jurisdicción nacional, puertos y aeródromos, mediante el control y seguimiento del tráfico marítimo y de aeronaves.
a.3) Usos previstos: Actuaciones en el marco de la seguridad pública y apoyo a las investigaciones policiales.

b) Origen de los datos:

b.1) Colectivo: Propietarios y usuarios de embarcaciones y aeronaves, y propietarios y gestores de instalaciones portuarias y de aeródromos.
b.2) Procedencia y procedimiento de recogida: Manualmente o mediante incorporación automática de datos provenientes de otras basas de datos con finalidad similar, por las unidades de la Guardia Civil a partir de formularios o documentos en soporte papel, informático o telemático.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF/NIE/pasaporte, nombre y apellidos, fecha y lugar de nacimiento, nacionalidad, sexo, dirección postal, dirección de correo electrónico y teléfono.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas: Autoridades judiciales, Ministerio Fiscal, otras Fuerzas y Cuerpos de Seguridad, Agencia Tributaria y aquellas otras necesarias en virtud de la cooperación y coordinación de órganos de la Administración y judiciales a nivel nacional, a tenor de lo establecido en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo; disposición adicional 1.ª de la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, y de conformidad con los artículos 11 y 21 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países: A oficiales de enlace extranjeros en materia fiscal, aduanera y fronteriza y organismos internacionales, en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Olaf, Sistema de Información Schengen, Organización Mundial de Aduanas y Unión Europea).

f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Servicio Fiscal, calle Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

9. FICHERO: EXÁMENES DE OPOSICIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Exámenes de oposiciones.

a.2) Finalidad: Gestionar las oposiciones de ingreso y promoción interna del Cuerpo de la Guardia Civil.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Cualquier persona que solicite participar en oposiciones para ingreso o procesos de promoción interna en el Cuerpo de la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante la grabación de los datos que figuran en las solicitudes y de los resultados de las pruebas.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos de infracciones penales o administrativas: Infracciones penales.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal y teléfono.
Datos de características personales.
Datos académicos y profesionales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Registro Central de Penados y Rebeldes (Ministerio de Justicia), al Instituto Nacional de la Administración Pública (Ministerio de la Presidencia) y a la Dirección General de Tráfico (Ministerio del Interior), bajo autorización expresa del personal opositor al objeto de obtener si los mismos poseen o no antecedentes penales, nacionalidad española y estén en posesión del permiso de conducción de la clase que se determine, respectivamente; al Ministerio de Defensa, al objeto de obtención como méritos, de los tiempos servidos tanto en la Guardia Civil, como en las Fuerzas Armadas, previo consentimiento expreso del personal opositor.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil). C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Enseñanza, c/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

10. FICHERO: EXPEDIENTES ACADÉMICOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Expedientes académicos.
a.2) Finalidad: Gestión de los expedientes académicos del personal de la Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal del Cuerpo de la Guardia Civil hasta su pase a retirado.
b.2) Procedencia y procedimiento de recogida: De los datos obtenidos dentro del sistema de enseñanza del Cuerpo y los aportados por el interesado del sistema educativo general y los profesionales, mediante formularios en soporte papel o magnético de otros ficheros de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil), creados para la selección y gestión de recursos humanos y de las publicaciones oficiales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.
Datos de características personales.
Datos académicos y profesionales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Enseñanza, c/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

11. FICHERO: GCVOX.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: GCVOX.
a.2) Finalidad: Colaborar con la Administración de Justicia mediante la identificación de las personas por los registros de voz.
a.3) Usos previstos: Investigaciones policiales de la Guardia Civil.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Detenidos por la presunta comisión de hechos delictivos; personas anónimas cuyas voces tienen relación con la presunta comisión de hechos delictivos; personas cuyas voces son captadas por videocámaras reguladas por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y las que las autoridades con competencia legal determinen; personas investigadas relacionadas con la presunta comisión de hechos delictivos; personas que donan su voz voluntariamente o donantes de voces de terceros con potestad legal para hacerlo, con fines de investigación o protección policial.

b.2) Procedencia y procedimiento de recogida: A través de la grabación de la reseña técnica de voz de los detenidos; mediante copia de grabaciones efectuadas en investigaciones policiales; mediante copia de la voz anónima relacionada con una supuesta comisión de hechos delictivos; mediante copia de las voces registradas por videocámaras reguladas por la referida Ley Orgánica 4/1997, de 4 de agosto.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, imagen/voz, permiso de conducción, carta nacional de identidad, pasaporte, permiso de residencia, carnet profesional.

Datos de características personales.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Pueden cederse datos a otras Fuerzas y Cuerpos de Seguridad, a los Órganos Jurisdiccionales y al Ministerio Fiscal, en virtud de lo establecido en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, y de conformidad con los artículos 11.2. a) y d) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados o convenios en los que España sea parte (Interpol, Europol, Sistema de Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), c/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Policía Judicial, c/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

12. FICHERO: GESTIÓN DE DATOS ACADÉMICOS.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Gestión de datos académicos.

a.2) Finalidad: Realizar un seguimiento de los alumnos inscritos en los distintos procesos formativos de la Jefatura de Enseñanza, centros docentes de la Guardia Civil y Centro Universitario de la Guardia Civil (CUGC), así como en el Sistema de Teleformación, tanto a nivel de identificación personal como de la evolución académica registrada durante todos los cursos realizados en cada uno de ellos. Gestionar al personal docente colaborador que imparten docencia en las actividades académicas que organiza los centros docentes de la Guardia Civil y el CUGC.

a.3) Usos previstos: Administrativo.

b) Origen de los datos:

b.1) Colectivo: Alumnos y profesorado de cada centro.
b.2) Procedencia y procedimiento de recogida: Se recogen del propio interesado, o su representante legal, de publicaciones oficiales y de fuentes accesibles al público mediante formularios en soporte papel y magnético de otros ficheros de la Dirección General de la Guardia Civil, creados para la selección y gestión de recursos humanos.
c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono, imagen/voz y número de registro de personal.
Datos de características personales: Datos de familia, fecha de nacimiento, lugar de nacimiento, nacionalidad, edad, sexo, y características físicas o antropométricas.
Datos de circunstancias sociales: Situación familiar.
Datos académicos y profesionales: Formación, titulaciones, historial del estudiante, experiencia profesional.
Datos de detalle de empleo: Cuerpo/Escala, categoría/grado, puesto de trabajo.
Datos bancarios.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas: A los órganos competentes en materia de intervención y control de las cuentas públicas, a la Agencia Estatal de Administración Tributaria y a las entidades financieras en la que se efectúe el correspondiente abono, así como a las Universidades a las cuales el CUGC se adscriba.
e) Transferencias internacionales de datos previstas a terceros países: No se prevén.
f) Órgano responsable del fichero: Dirección General de la Guardia Civil. Calle Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Jefatura de Enseñanza, calle Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

13. FICHERO: INCOMPATIBILIDADES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Incompatibilidades.
a.2) Finalidad: Gestión y control de las compatibilidades del personal de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) para desempeñar otra actividad.
a.3) Usos previstos: Administrativo.
b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal perteneciente a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, en su solicitud de compatibilidad.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.
Datos de circunstancias sociales.
Datos acádemicos y profesionales.

Datos de detalle de empleo.
Datos economico-financieros.
Datos de información comercial.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio del Interior y al Ministerio de Administraciones Públicas, en virtud de la Ley 53/1984, de 26 de diciembre, de incompatibilidades del personal al servicio de las Administraciones Públicas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Subdirección General de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

14. FICHERO: INTPOL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: INTPOL.

a.2) Finalidad: Mantenimiento de la seguridad pública mediante el control de personas y hechos de interés policial, relacionados con la prevención o investigación de infracciones penales o para el cumplimiento de las leyes cuya observancia afecta a la Guardia Civil.

a.3) Usos previstos: Actuaciones en el marco de la seguridad pública e investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas incursas en procedimientos judiciales, investigaciones o actuaciones realizadas o conocidas por la Guardia Civil en el marco de sus competencias.

b.2) Procedencia y procedimiento de recogida: Los datos se obtienen de las diligencias realizadas con ocasión de actuaciones policiales, reseñas de detenidos, denuncias recibidas y órdenes judiciales de requisitoria, a través de formularios en soporte papel e informático, al amparo de lo establecido en la Ley Orgánica 2/1986, de 13 de marzo, Ley de Enjuiciamiento Criminal, la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, y demás Leyes cuyo cumplimiento afecta a las competencias de la Guardia Civil.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos relativos a la comisión de infracciones penales y administrativas: Infracciones penales y administrativas.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos, domicilio, n.º de Seguridad Social o mutualidad, teléfono, correo electrónico, firma/huella digitalizada, imagen/voz, marcas físicas, fórmula decadactilar y cualquier otro dato que pueda ser identificativos de la persona.
Datos de características personales.
Datos académicos y profesionales.
Datos de circunstancias sociales.

Datos de información comercial.
Datos económico-financieros y de seguros.
Datos de transacciones de bienes y servicios.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Autoridades Judiciales y Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre; a otras Fuerzas y Cuerpos de Seguridad, Instituciones Penitenciarias y organismos nacionales de coordinación o con competencias en materia de seguridad pública, Defensa Nacional o que versen sobre las mismas materias en las que la Guardia Civil dispone de atribuciones, conforme a lo establecido en los artículos 11.2.a) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre, en cumplimiento de los principios de colaboración, mutuo auxilio y cooperación e información recíprocas que establece la Ley Orgánica 2/1986, de 13 de marzo. A empresas de Seguridad Privada en el marco de las actividades de auxilio y colaboración con las Fuerzas de Seguridad en los casos en que su actividad esté directamente relacionada con la seguridad pública o la Defensa Nacional, al amparo de lo establecido en el artículo 11.2. a) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros, en virtud de los acuerdos, tratados y convenios internacionales legalmente vinculantes para España en los términos previstos en la Constitución española, y la transferencia por tratados o convenios en los que sea parte España, conforme a lo establecido en el artículo 34.a) de la Ley Orgánica 15/1999, de 13 de diciembre.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil). C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Policía Judicial, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

15. FICHERO: PRESTACIÓN DEL SERVICIO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Prestación del servicio.

a.2) Finalidad: Facilitar la planificación y el nombramiento del servicio prestado por el personal del Cuerpo en cumplimiento de las funciones y cometidos de seguridad pública encomendados a la Guardia Civil, así como aquellas actividades de formación continua computables a efectos del servicio; automatizar los sistemas de registro y archivo de los servicios y el cómputo de los esfuerzos desarrollados por el personal y gestionar la reclamación de las compensaciones de los sobreesfuerzos y el control de los servicios prestados por el personal.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal de la Guardia Civil o que presta servicio para la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Datos incorporados telemáticamente del sistema de Recursos Humanos de la Guardia Civil y datos introducidos por los mandos de las Unidades al efectuar la planificación y el nombramiento del servicio, complementados por los aportados por el propio personal que prestó el servicio, en soporte papel y soporte informático.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, nombre y apellidos, y número de identificación profesional.
Datos de características personales.
Datos de circunstancias sociales.
Datos de detalle de empleo.
Datos económico-financieros y de seguros.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Estado Mayor, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

16. FICHERO: PSICOLOGÍA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Psicología.
a.2) Finalidad: Gestión del historial psicológico relacionado con la salud mental de los componentes del Cuerpo y Guardias Alumnos. Gestión de los datos relacionados con los procesos de selección para ingreso, especialización y promoción. Gestión de los expedientes del personal del Cuerpo, Militares, Funcionarios Civiles y Familiares que participen en programas preventivos o de intervención psicoterapéutica.
a.3) Usos previstos: Administrativo, de investigación y planes preventivos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal del Cuerpo de la Guardia Civil y aspirantes a ingreso en el mismo. Militares, funcionarios civiles y familiares que participen en programas preventivos o de intervención psicoterapéutica.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante encuestas, entrevistas y formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos.
Datos de características personales.
Datos de circunstancias sociales.
Datos académicos y profesionales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los Órganos competentes, en virtud de lo dispuesto en los artículos 49 y 55 de la Ley 42/1999, de 25 de noviembre, de Régimen del Personal del Cuerpo de la Guardia Civil y su normativa de desarrollo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Asistencia al Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

17. FICHERO: RECURSOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Recursos.

a.2) Finalidad: Gestión y control de los recursos tramitados al amparo de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; al derecho de petición, al amparo de la Ley orgánica 4/2001, de 12 de noviembre, reguladora del derecho de petición, en el ámbito de la Guardia Civil; y a las quejas formuladas al amparo del artículo 100 de la Ley 42/1999, de 25 de noviembre, del Régimen del Personal del Cuerpo de la Guardia Civil, y del artículo 33 de la Ley Orgánica 11/2007, de 22 de octubre, reguladora de los derechos y deberes de los miembros de la Guardia Civil.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal de la Guardia Civil y otros que recurran las resoluciones adoptadas por la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, contenido en la documentación obrante en el expediente del recurso interpuesto.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal y teléfono.
Datos de características personales.
Datos de circunstancias sociales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio de Defensa y a otros órganos del Ministerio del Interior, en materia de Responsabilidad patrimonial en el ejercicio de las competencias del artículo 142.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común; Al Consejo de Estado, en virtud de lo previsto en los apartados nueve y trece del artículo 22 de la Ley Orgánica 3/1980, de 22 de abril, reguladora de dicha institución; A órganos judiciales en cumplimiento de lo previsto en el artículo 48 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Subdirección General de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

18. FICHERO: REGISTRO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro.

a.2) Finalidad: Registro de entrada y salida de los documentos tramitados por las unidades de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil), conforme establece el art. 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas incluidas en los documentos tramitados.

b.2) Procedencia y procedimiento de recogida: Del propio interesado y de otros órganos oficiales, mediante la transmisión electrónica de datos, a través de los documentos de entrada o salida; utilizados en soporte papel o vía telemática.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.

Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la persona, órgano o unidad destinataria de la misma.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Secretaría de Despacho, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

19. FICHERO: REGISTRO DE CONDUCTORES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro de conductores.

a.2) Finalidad: Gestión de permisos de conducción y accidentes del personal de la Guardia Civil; y personal civil y de las Fuerzas Armadas adscritos a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: El personal adscrito a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) y terceras personas implicadas en accidentes con vehículos de la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Del propio interesado mediante formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos de infracciones penales o administrativas: Infracciones penales y administrativas.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos, y teléfono.
Datos de características personales.
Datos de circunstancias sociales.
Datos académicos y profesionales.
Datos de detalle de empleo.
Datos sobre circunstancias del accidente.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la Dirección General de Tráfico, cuando la comunicación se realice para el ejercicio de las competencias atribuidas en virtud del artículo 21 de la Ley Orgánica 15/1999, de 13 de enero, en relación con el artículo 6 del Real Decreto Legislativo 339/1990, de 2 de marzo, por el que se aprueba el Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. A determinados Centros de Reconocimiento de Conductores y a las compañías de seguros en caso de accidente de tráfico con un vehículo de la Guardia Civil, al amparo del artículo 11.2.c) de la Ley Orgánica 15/1999, de 13 de diciembre, en relación con el artículo Artículo 7 del Real Decreto Legislativo 8/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de los Servicios de Apoyo, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

20. FICHERO: SEDEX.
(Suprimido)
Destino de los datos: Destrucción.

21. FICHERO: TARJETAS DE IDENTIFICACIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Tarjetas de identificación.
a.2) Finalidad: Control y gestión de las tarjetas de identificación del personal adscrito temporal o permanentemente a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) y familiares con derecho a las mismas.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal adscrito temporal o permanentemente a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) y familiares con derecho a las mismas.
b.2) Procedencia y procedimiento de recogida: El propio interesado o su representante legal, a través de formularios y de las publicaciones oficiales en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, huella/firma digitalizada, imagen/voz, número de registro de personal, y firma electrónica.
Datos de características personales.
Datos de características sociales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevén cesiones de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Subdirección General de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

22. FICHERO: VESTUARIO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Vestuario.
a.2) Finalidad: Gestión de prendas de uniformidad y almacén de vestuario, así como el control de prendas de uniformidad entregadas.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: El personal adscrito a la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil).
b.2) Procedencia y procedimiento de recogida: Del propio interesado mediante fichas y formularios que proporciona en soporte papel y electrónico.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, y número de registro de personal.
Datos características personales.
Datos de circunstancias sociales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de los Servicios de Apoyo, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

23. FICHERO: ACCESDOC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ACCESDOC.
a.2) Finalidad: Control de acceso y consulta a documentos en los archivos de gestión.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Solicitantes de acceso a documentos producidos, reunidos o conservados por la Guardia Civil en el ejercicio de sus competencias y titulares de los documentos a los que se pretende acceder.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, en soporte papel (impreso solicitud de acceso).

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, Nombre y apellidos.
Datos académicos y profesionales.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), Sección del Archivo General del Ministerio del Interior en la Guardia Civil, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

24. FICHERO: AFECTADOS POR ATENTADOS DE TERRORISMO EN EL ÁMBITO DE LA GUARDIA CIVIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Afectados por atentados de terrorismo en el ámbito de la Guardia Civil.

a.2) Finalidad: Disponer de una información actualizada y completa sobre todos los guardias civiles y familiares de los mismos, afectados por atentados terroristas, desde 1968, para informarles de los derechos y beneficios a los que pudieran optar.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Componentes de la Guardia Civil y sus familiares que hayan sido víctimas de atentado terrorista, desde el año 1968.

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante formularios.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.

Datos de carácter identificativo: DNI/NIF, número de Seguridad Social/Mutualidad, nombre y apellidos, dirección postal, teléfono y tarjeta sanitaria.

Datos de características personales.

Datos de circunstancias sociales.

Datos de detalle de empleo.

Datos económico-financieros y de seguros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la Dirección General de Apoyo a Víctimas del Terrorismo, del Ministerio del Interior, en virtud de la Ley 32/1999, de 8 de octubre, de solidaridad con las víctimas del terrorismo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Asistencia al Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

25. FICHERO: AYUDAS ACCIÓN SOCIAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Ayudas acción social.
a.2) Finalidad: Gestión de los planes anuales de Acción Social que se desarrollan en el ámbito de la Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal que solicita la adjudicación de una ayuda determinada y que se encuentra dentro de los beneficiarios establecidos en los Planes de Acción Social aprobados anualmente.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante formularios en soporte papel y su posterior grabación en la base de datos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos de carácter identificativo: DNI/NIF, n.º S.S./Mutualidad, nombre y apellidos, dirección postal, teléfono y correo electrónico.
Datos de características personales.
Datos académicos y profesionales.
Datos de detalle de empleo.
Datos económico-financieros y de seguros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Agencias de viajes, con el consentimiento del interesado, con las que se mantienen acuerdo, Intervención General de la Administración del Estado, Tribunal de Cuentas, Agencias Estatal de Administración Tributaria y a las entidades financieras correspondientes.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Asistencia al Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

26. FICHERO: CENTRO DE ACTIVIDADES FÍSICAS (GIMNASIO).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centro de actividades físicas (gimnasio).
a.2) Finalidad: Tratamiento, programación y gestión del Registro de usuarios y monitores de los gimnasios de la Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que soliciten la inscripción al gimnasio y que se encuentren dentro de los usuarios autorizados.

b.2) Procedencia y procedimiento de recogida: A través del propio interesado, mediante formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, y teléfono.
Datos de características personales.
Datos de detalles de empleo.
Datos de circunstancias sociales.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), Subdirección General de Personal (Jefatura de Asistencia al Personal), C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

27. FICHERO: CENTROS DE EDUCACIÓN INFANTIL DE PRIMER CICLO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centros de educación infantil de primer ciclo.
a.2) Finalidad: Tratamiento y resolución del proceso de solicitud y adjudicación de plazas en los Centros de Educación Infantil de primer ciclo de la Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Alumnos, padres, tutores o representantes legales que soliciten plaza en los Centros de Educación Infantil de primer ciclo de la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, imagen, teléfono y firma.
Datos de características personales.
Datos de detalles de empleo.
Datos de circunstancias sociales.
Datos económico-financieros y de seguros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la empresa adjudicataria del servicio.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), Jefatura de Asistencia al Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

28. FICHERO: CUADERNOS DE LA GUARDIA CIVIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Cuadernos de la Guardia Civil.

a.2) Finalidad: Control y gestión de los suscriptores, colaboradores y autores de la publicación de la Guardia Civil «Cuadernos de la Guardia Civil».

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas suscritas a la publicación «Cuadernos de la Guardia Civil» y colaboradores y autores.

b.2) Procedencia y procedimiento de recogida: El propio interesado a través de formularios.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono.
Datos de detalle de empleo.
Datos económico-financieros y de seguros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A entidades financieras para el cobro del precio de suscripción y para el abono de sus honorarios a los colaboradores, así como en su caso, a los órganos competentes para la fiscalización del gasto.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Unidad de Coordinación - Centro de Análisis y Prospectiva, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

29. FICHERO: ECOFIN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ECOFIN.
a.2) Finalidad: Administración y coordinación de los recursos financieros y patrimoniales, el seguimiento de la ejecución del presupuesto y registro contable, gestión y seguimiento de los procesos de contratación, la coordinación de la actividad de las Unidades de Gestión Económica y la gestión de indemnizaciones por razón del servicio, traslados y asistencias.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas o jurídicas que mantienen obligaciones contractuales con la Guardia Civil; personal dependiente de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil) y externos que tengan derecho a indemnizaciones.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante formularios y facturas o transmisión electrónica de datos, en soporte papel o informático.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal y teléfono.
Datos de detalle de empleo.
Datos de información comercial.
Datos económico-financieros y de seguros.
Datos de transacciones.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la Administración Tributaria, en virtud del artículo 29 de la Ley 58/2003, de 17 de diciembre, General Tributaria; a las Intervenciones delegadas, en virtud de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, Real Decreto 640/1987, de 8 de mayo, sobre pagos librados «a justificar», y Real Decreto 725/1989, de 16 de junio, sobre anticipos de caja fija. A las entidades financieras que deban proceder a la transferencia monetaria, con cargo a las cuentas corrientes de las Unidades.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Asuntos Económicos, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

30. FICHERO: EXPEDIENTES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Expedientes.
a.2) Finalidad: Control y gestión de los expedientes que deben confeccionarse para la gestión de los Recursos Humanos de la Guardia Civil, excepto los disciplinarios.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal dependiente de la Dirección General de la Policía y de la Guardia Civil en el ámbito de la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Del fichero de Gestión de Personal en cuanto a los datos identificativos de la persona, del propio interesado o su representante legal y de las publicaciones oficiales relativas a los datos de la resolución de los expedientes.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos relativos a la comisión de infracciones penales y administrativas: Infracciones penales y administrativas.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos de la persona.
Datos de detalles de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), Jefatura de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

31. FICHERO: GESTIÓN DE APARCAMIENTOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión de aparcamientos.
a.2) Finalidad: Tratamiento, programación y gestión del Registro de usuarios residentes como no residentes y vehículos oficiales de los aparcamientos de la Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal de la Guardia Civil, personal de las Fuerzas Armadas y funcionarios que se encuentren destinados en la Dirección General de la Policía y de la Guardia Civil (Ámbito de la Guardia Civil).
b.2) Procedencia y procedimiento de recogida: A través del propio interesado, mediante formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección (postal, electrónica), teléfono, matrículas de vehículos.
Datos de características personales.
Datos de detalles de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), Subdirección General de Personal (Servicio de Asuntos Generales), C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

32. FICHERO: HOJA DE SERVICIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Hoja de servicios.
a.2) Finalidad: Gestionar la Hoja de Servicios del personal del Cuerpo de la Guardia Civil, en virtud de lo dispuesto en la Ley 42/1999, de 25 de noviembre, de Régimen del Personal del Cuerpo de la Guardia Civil (art. 45.a), y en la Orden Ministerial número 50/1997, de 3 de abril, por la que se aprueba el modelo de Hoja de Servicios del personal militar de carrera y de empleo de la categoría de Oficial. Que incluye:

Hoja General de servicios.
Hoja Anual de servicios.
Hoja Resumen.
Certificaciones.
Cómputo de tiempos a efectos de servicio, trienios y derechos pasivos.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal dependiente de la Dirección General de la Policía y de la Guardia Civil (ámbito de la Guardia Civil).
b.2) Procedencia y procedimiento de recogida: Del fichero de Gestión de Personal en cuanto a los datos identificativos de la persona, del propio interesado o su representante legal y de las publicaciones oficiales de cada una de las vicisitudes profesionales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales y administrativas.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos de la persona, fotografía.
Datos de características personales.
Datos de circunstancias sociales.
Datos académicos y profesionales.
Datos de detalles de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio de Defensa y al Ministerio del Interior en las materias previstas por la Ley 42/1999, de 25 de noviembre, de Régimen del Personal del Cuerpo de la Guardia Civil, de acuerdo con la distribución de competencias regulada en la Ley Orgánica 2/1986, de 13 de marzo, y Real Decreto Legislativo 670/1987, de Clases Pasivas del Estado. Al Defensor del Pueblo, Ministerio Fiscal o los Jueces y Tribunales en ejercicio de las competencias que tienen atribuidas, de conformidad con el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), Jefatura de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

33. FICHERO: REGISTRO DE ASOCIACIONES PROFESIONALES DE GUARDIAS CIVILES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro de asociaciones profesionales de Guardias Civiles.

a.2) Finalidad: Gestión del Registro de Asociaciones Profesionales de Guardias Civiles.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Miembros de los órganos de gobierno y represtación, así como representantes que figuren como tales de acuerdo al procedimiento establecido en los Estatutos de las Asociaciones Profesionales de Guardias Civiles que solicitan ser inscritas en el Registro de Asociaciones Profesionales de Guardias Civiles.

b.2) Procedencia y procedimiento de recogida: A través de la documentación que acompaña a la solicitud de inscripción realizadas por Asociaciones Profesionales de Guardias Civiles (estatutos y acta fundacional u otros documentos que sean presentados).

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos de carácter identificativo: DNI/NIF, nombre y apellidos, y el cargo directivo o de representante que desempeña en la Asociación.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil

(Ámbito Guardia Civil), Subdirección General de Personal (Servicio de Asuntos Generales), C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

34. FICHERO: RETRIBUCIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Retribuciones.

a.2) Finalidad: Gestión de los haberes que la Guardia Civil abona; Cálculo mensual del IRPF y obtención del certificado anual de retenciones para la Agencia Estatal de Administración Tributaria; Gestión económica de las medallas pensionadas del personal no incluido en la nómina de la Guardia Civil; Control y seguimiento de los recursos presentados en relación con las retribuciones del personal de la Guardia Civil; Gestión de las retenciones judiciales; Obtención del fichero anual de planes de pensiones; Gestión de los haberes abonados con cargo a los créditos de la Dirección General de Tráfico, gestión de las retribuciones abonadas en virtud de los convenios celebrados con diversas Comunidades Autónomas y otras entidades de derecho público.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal del Cuerpo de la Guardia Civil, del Ministerio de Defensa, laboral y funcionarios, destinados o adscritos a la Guardia Civil; y personal no incluido en la nómina de la Guardia Civil con derecho a pensión por las medallas concedidas.

b.2) Procedencia y procedimiento de recogida: De las publicaciones oficiales, del propio interesado o su representante legal, mediante formularios en soporte papel o la cumplimentación del contrato correspondiente.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos especialmente protegidos: Afiliación sindical.
– otros datos especialmente protegidos: Salud.
– datos de carácter identificativo: DNI/NIF, nombre y apellidos, número de Seguridad Social/Mutualidad, dirección postal, teléfono y número de registro de personal.
– datos de características personales.
– datos de circunstancias sociales.
– datos académicos y profesionales.
– datos de detalle de empleo.
– datos económico-financieros y de seguros.
– datos de transacciones.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio de Hacienda y Administraciones Públicas, en virtud de la Ley 40/1998, de 9 de diciembre, del Impuesto de la Renta de las Personas Físicas y del Real Decreto 214/1999, del 5 de febrero, del Reglamento del Impuesto de la Renta sobre Personas Físicas; al Instituto Social de las Fuerzas Armadas (ISFAS), Ministerio de Defensa, Dirección General de Tráfico, Centro Nacional de Inteligencia, Pagadurías de diversas Comunidades Autónomas, en virtud de lo establecido en el artículo 21.2 de la Ley Orgánica 15/1999, de 13 de diciembre; a la Mutualidad de Funcionarios de la Administración Civil de Estado (MUFACE), en virtud de la Ley 29/1975, de 27 de junio, sobre Seguridad Social de Funcionarios Civiles del Estado y a la Tesorería General de la Seguridad Social, en virtud de Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto refundido de

la Ley General de la Seguridad Social; a las entidades financieras donde se produzcan los abonos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se prevén.

f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle de Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Jefatura de Personal, calle de Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

35. FICHERO: RÉGIMEN DISCIPLINARIO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Régimen disciplinario.

a.2) Finalidad: Control y seguimiento de los expedientes disciplinarios y procedimientos penales abiertos a personal del Cuerpo de la Guardia Civil.

a.3) Usos previstos: Administrativo y régimen disciplinario.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Todos los componentes de la Dirección General de la Policía y de la Guardia Civil (ámbito de la Guardia Civil).

b.2) Procedencia y procedimiento de recogida: Del propio interesado, de Unidades del Cuerpo de la Guardia Civil, de publicaciones oficiales, de fuentes accesibles al público y de la instrucción y resolución de los procedimientos administrativos y/o judiciales, mediante formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales y administrativas.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, y número de registro personal.

Datos de características personales.

Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio Fiscal, Jueces y Tribunales, de conformidad con el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

36. FICHERO: VIDEOVIGILANCIA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Videovigilancia.
a.2) Finalidad: Seguridad de los acuartelamientos de la Guardia Civil y de los edificios, bases, instalaciones y centros vigilados por la Guardia Civil.
a.3) Usos previstos: Seguridad.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que se encuentren en zonas videovigiladas de los acuartelamientos de la Guardia Civil o de los edificios, bases, instalaciones y centros vigilados por la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Circuito cerrado de televisión.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos de carácter identificativo: Imagen/voz.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Fuerzas y Cuerpos de Seguridad para sus funciones de protección de la seguridad pública, conforme a lo establecido en el artículo 22.2 de Ley Orgánica 15/1999, de 13 de diciembre, en cumplimiento de los principios de colaboración, mutuo auxilio y cooperación e información recíprocas que establece la Ley Orgánica 2/1986, de 13 de marzo.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Unidades Especiales y Reserva, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

37. FICHERO: ADNIC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ADNIC.
a.2) Finalidad: Cooperar con la Administración de Justicia mediante la identificación genética de vestigios biológicos y la identificación genética de muestras de origen conocido, en investigaciones realizadas por el Cuerpo de la Guardia Civil.
a.3) Usos previstos: Investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas que determinen las autoridades que tienen atribuidas competencias por ley para exigir el tratamiento de los datos, las que expresamente lo requieran y estén relacionadas con algún hecho y aquéllas a las que pertenecen los vestigios biológicos relacionados con los hechos.
b.2) Procedencia y procedimiento de recogida: Facilitados por el propio interesado, otras personas físicas distintas del afectado (con sujeción a lo expresado en el párrafo anterior y al

amparo de la Ley de Enjuiciamiento Criminal), o su representante y las administraciones públicas, mediante formulario, transmisión electrónica de datos/Internet y análisis de laboratorio de ADN en soporte papel, vía telemática o soporte informático o magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono, datos genéticos con fines identificativos y patrón de ADN, otros documentos identificativos.
Datos de características personales.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Pueden cederse datos a otras Fuerzas y Cuerpos de Seguridad, a los Órganos Jurisdiccionales y al Ministerio Fiscal, en virtud de lo establecido en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, artículos 11.2 a) y d) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre. A la Secretaría de Estado de Seguridad, en virtud de lo establecido en la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados o convenios en los que España sea parte (Interpol, Europol, Sistema de Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Policía Judicial, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

38. FICHERO: ARMAS.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Armas.
a.2) Finalidad: Mantenimiento de la seguridad pública mediante el control de las materias tipificadas en el Reglamento de Armas, aprobado por el Real Decreto 137/1993, de 29 de enero, Reglamento de Explosivos, aprobado por el Real Decreto 230/1998, de 16 de febrero, y Reglamento de artículos pirotécnicos y cartuchería, aprobado por el Real Decreto 989/2015, de 30 de octubre.
a.3) Usos previstos: Control de las materias reglamentadas (armas, explosivos, artículos pirotécnicos y cartuchería), gestión de los procedimientos de concesión, renovación y revocación de licencias, permisos y autorizaciones, procedimientos sancionadores, elaboración de estadísticas y análisis de los datos para detección de cualquier circunstancia de interés policial, como las relacionadas con el tráfico o empleo ilícito, pérdida o sustracción de armas o documentaciones, decomisos, enajenaciones o cualesquiera otras que afectaran a su tenencia y uso, a efectos de descubrimiento y persecución de actos delictivos o infracciones.

b) Origen de los datos:

b.1) Colectivo: Personas físicas o jurídicas que solicitan o realizan trámites administrativos relacionados con la normativa de armas, explosivos y de artículos

pirotécnicos y cartuchería, así como los incursos en procedimientos sancionadores relacionados con la materia.

b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal mediante formularios, impresos y documentación, procesando los datos en el fichero informático directamente por las distintas unidades interventoras de armas y explosivos a todos los niveles.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud (Informe de aptitud psicofísica).

Datos de infracciones penales o administrativas: Infracciones penales y administrativas e informe de conducta y antecedentes.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal y teléfono, dirección de correo electrónico y otros documentos identificativos.

Datos de características personales: Datos de filiación, fecha, lugar y país de nacimiento, edad, sexo, y nacionalidad.

Datos de circunstancias sociales: Pertenencia a clubes, asociaciones, etc. Categoría deportiva.

Datos de detalle de empleo: Cuerpo, escala, categoría, grado, puesto de trabajo, situación administrativa.

Datos de información comercial: Establecimientos relacionados con la fabricación, adquisición, almacenamiento, circulación, transporte, comercio, tenencia y uso de armas, sus municiones, explosivos y artículos pirotécnicos.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas: A las Autoridades Judiciales y Ministerio Fiscal, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de diciembre. A otras Fuerzas y Cuerpos de Seguridad y organismos nacionales, conforme a lo establecido en el artículo 11.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, y la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países: A organismos internacionales y países extranjeros, en los términos establecidos en los acuerdos suscritos por España (Protocolo contra la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, Instrumento internacional sobre marcado y rastreo de armas pequeñas y ligeras, Directiva 91/477/CEE, del Consejo, de 18 de junio de 1991, sobre el control de la adquisición y tenencia de armas, modificada por la Directiva 2008/51/CE, del Parlamento Europeo y del Consejo, de 21 de mayo de 2008, Directiva 93/15/CEE, del Consejo, de 5 de abril de 1993, relativa a la armonización de las disposiciones sobre la puesta en el mercado y el control de los explosivos con fines civiles, Directiva 2008/43/CE, de la Comisión, de 4 de abril de 2008, por la que se establece, con arreglo a la Directiva 93/15/CEE, del Consejo, un sistema de identificación y trazabilidad de explosivos con fines civiles, Directiva 2012/4/UE, de la Comisión, de 22 de febrero de 2012, que modifica la Directiva 2008/43/CE, Directiva 2007/23/CE, del Parlamento Europeo y del Consejo, de 23 de mayo de 2007, sobre la puesta en el mercado de artículos pirotécnicos, Reglamento (UE) 98/2013, del Parlamento Europeo y del Consejo, de 15 de enero de 2013, sobre la comercialización y la utilización de precursores de explosivos, acuerdos bilaterales, Interpol, Europol, Sistema Información Schengen, Unión Europea y convenios bilaterales).

f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección de la Guardia Civil-Intervención Central de Armas y Explosivos, calle Batalla de Salado, 32, 28045 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

39. FICHERO: BDRA

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: BDRA.
a.2) Finalidad: Base de datos patrón que permite comparar calidad y eficacia de sistemas de reconocimiento de voces. Su finalidad es científica.
a.3) Usos previstos: Evaluación de sistemas de reconocimiento de voz y desarrollo de tecnologías en dicho ámbito.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Voces de las personas que utilizan medios de comunicación intervenidos por orden judicial. Voces donadas voluntariamente para investigación científica. Voces obtenidas a través de medios de comunicación públicos.
b.2) Procedencia y procedimiento de recogida: A través de las escuchas telefónicas llevadas a cabo por los distintos Servicios de la Dirección General de la Policía y de la Guardia Civil (ámbito Guardia Civil), autorizados judicialmente para su inclusión en esta base de datos y a través de grabaciones realizadas con donantes de voz.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Imagen/voz.
Datos de características personales.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Pueden cederse datos a otras Fuerzas y Cuerpos de Seguridad, a los Órganos Jurisdiccionales y al Ministerio Fiscal, en virtud de lo establecido en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, y de conformidad con los artículos 11.2 a) y d) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre. Debido a su finalidad científica, también se prevé la cesión de voz a investigadores de centros universitarios y organismos de investigación que colaboren formalmente con la Guardia Civil en el estudio y desarrollo de tecnologías de biometría del habla, al amparo de los artículos 3.2.j) y 1.2 c) de la Ley Orgánica 11/1983, de 25 de agosto, de Reforma Universitaria y el 6.2.c) de la Ley Orgánica 2/1986, de 13 de marzo.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en tratados y convenios en los que España sea parte (Interpol, Europol, Sistema de Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Policía Judicial, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

40. FICHERO: CONSEJO DE LA GUARDIA CIVIL.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Consejo de la Guardia Civil.
a.2) Finalidad: Gestión del procedimiento de elección de los representantes de los miembros del Cuerpo en el Consejo de la Guardia Civil, y de las propuestas o sugerencias

planteadas por los guardias civiles al citado Consejo y a la Oficina de Atención al Guardia Civil, así como la gestión de la elaboración y difusión de las actas de las sesiones del Consejo, y de las reuniones de las Comisiones y Grupos de Trabajo.

a.3) Usos previstos: Administrativo.

b) Origen de los datos:

b.1) Colectivo: Personal de la Guardia Civil, participantes en los procesos de elección del Consejo de la Guardia Civil, conforme a la legislación que regule el proceso electoral (Representantes de la Administración, Delegados de las distintas Asociaciones Profesionales de la Guardia Civil, Censo electoral, Candidatos, Junta Electoral etc.), Vocales del Consejo y otro personal respecto de sus intervenciones en las sesiones de Pleno y de las Comisiones dependientes de aquél, así como todo aquél que dirija al Consejo o a la Oficina de Atención al Guardia Civil, cuestiones, propuestas o sugerencias.

b.2) Procedencia y procedimiento de recogida: Del propio interesado, en formularios, soporte papel y vía telemática. Del fichero de Gestión de Personal. De la Orden Comunicada del Ministro del Interior en cada convocatoria electoral, en la que se regule la composición de la Junta Electoral.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, dirección electrónica, teléfono, imagen/voz, número de registro personal y firma electrónica.

Datos de circunstancias sociales: Situación militar.

Datos de detalle del empleo: Cuerpo/Escala, categoría/grado, puesto de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Subdirección General de Personal, calle Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

41. FICHERO: FENIX.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: FENIX.

a.2) Finalidad: Identificación genética de personas desaparecidas y cadáveres sin identificar, con finalidad científica, de interés público y judicial.

a.3) Usos previstos: Investigaciones de la Guardia Civil.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas que voluntariamente deseen contribuir a la identificación de una persona y a las que las autoridades con competencia legal determinen; así como los restos humanos que deban identificarse.

b.2) Procedencia y procedimiento de recogida: Datos aportados por los interesados y otras personas físicas distintas del afectado (con sujeción a lo expresado en el párrafo anterior), administraciones públicas, recogidos mediante formularios, transmisión electrónica/ Internet o análisis del laboratorio. Utilizando soporte papel, informático o telemático. Actividades de identificación e investigación de restos humanos realizadas por el Cuerpo de la Guardia Civil.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos de carácter identificativo: DNI/NIF, nombre y apellidos, número de registro personal, perfil genético y otros documentos identificativos.
Datos relativos a la desaparición de la persona.
Datos relativos a la aparición de los restos/persona.
Datos de características personales.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Pueden cederse datos a otras Fuerzas y Cuerpos de Seguridad, a los Órganos Jurisdiccionales y al Ministerio Fiscal, en virtud de lo establecido en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, artículos 11.2. a) y d) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre. A la Secretaría de Estado de Seguridad, en virtud de lo establecido en la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A organismos internacionales y países extranjeros en los términos establecidos en los tratados y convenios en los que España sea parte (Interpol, Europol, Sistema de Información Schengen, Unión Europea y convenios bilaterales).
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Policía Judicial, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

42. FICHERO: GESTIÓN DE PERSONAL.

a) Identificación del fichero o tratamiento:

a.1) Identificación del fichero: Gestión de personal.
a.2) Finalidad: Gestión de los recursos humanos de la Dirección General de la Guardia Civil y del Centro Universitario de la Guardia Civil (CUGC).
a.3) Usos previstos: Administrativo, incluido el relativo a planes de pensiones y adopción de medidas de conciliación y agrupamiento familiar.

b) Origen de los datos:

b.1) Colectivo: La totalidad de los componentes y personas titulares de puestos de trabajo de la Dirección General de la Guardia Civil y del CUGC.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, de publicaciones oficiales, de fuentes accesibles al público y de la resolución de los expedientes respectivos, mediante formularios en soporte papel.

c) Estructura básica del fichero:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección habitual (vía, número y población), dirección electrónica, teléfono y número de registro personal.
Datos de circunstancias sociales: Estado civil, datos de familia.
Datos profesionales: Formación, titulaciones/experiencia profesional.
Datos de detalle de empleo: Cuerpo/Escala, categoría/grado y organización/funciones.

Datos económico-financieros y de seguros: Datos bancarios, Número de la Seguridad Social/Mutualidad.

Otros datos de personas vinculadas: DNI/NIF, nombre y apellidos, dirección habitual, dirección de correo electrónico, teléfonos de contacto y vínculo familiar de familiares designados para su pronta localización y aviso en supuestos de especial gravedad u otro tipo de contingencias.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas: Al Ministerio Fiscal, Jueces y Tribunales, de conformidad con los artículos 11 y 21 de la Ley Orgánica 15/1999, de 13 de diciembre. Al Instituto Social de la Fuerzas Armadas (ISFAS), en virtud de lo establecido en los artículos 3 y 4 del Real Decreto Legislativo 1/2000, de 9 de junio, por el que se aprueba el Texto Refundido de la Ley sobre Seguridad Social de las Fuerzas Armadas. A las entidades gestoras y depositarias, y a la Comisión de Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 19 de la Ley 61/2003, de 30 de diciembre de Presupuestos Generales del Estado para el año 2004 y el Texto Refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por el Real Decreto Legislativo 1/2002, de 29 de noviembre.

e) Transferencias internacionales de datos previstas a terceros países: No se prevén.

f) Órgano responsable del fichero: Dirección General de la Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Guardia Civil, Jefatura de Personal, calle Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

43. FICHERO: AÉREO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Aéreo.

a.2) Finalidad: Control administrativo y técnico del material del Servicio Aéreo de la Guardia Civil y del personal que vuele en sus aeronaves.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal que vuele en aeronaves del Servicio Aéreo de la Guardia Civil.

b.2) Procedencia y procedimiento de recogida: Grabación de los datos recogidos en las fichas de vuelo suministrados por el propio interesado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos.

Datos académicos y profesionales: Formación, titulaciones, historial del estudiante, experiencia profesional.

Datos de detalle de empleo: Cuerpo/Escala, Categoría/Grado, puesto de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Guardia Civil - Jefatura de Unidades Especiales y de Reserva, calle Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

44. FICHERO: RESIDENCIAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Residencias.
a.2) Finalidad: Gestión y control administrativo de las residencias y apartamentos ofertados por el Servicio de Acción Social de la Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal que solicita la adjudicación de una residencia o apartamento.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante formularios en soporte papel y su posterior grabación en la base de datos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono y correo electrónico.
Datos de características personales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Agencias y hoteles, con el consentimiento del interesado, con los que se mantienen acuerdos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A los Cuerpos Policiales armados de Francia, Italia y Portugal.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Asistencia al Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

45. FICHERO: REVISTA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Revista.
a.2) Finalidad: Control y gestión de los suscriptores, colaboradores y autores de la Revista Guardia Civil.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Componentes de la Guardia Civil y personal suscrito a la revista y colaboradores y autores.
b.2) Procedencia y procedimiento de recogida: El propio interesado a través de formularios.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono.
Datos de detalle de empleo.
Datos económico-financieros y de seguros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: no se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Unidad de Coordinación - ORIS, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

46. FICHERO: SANIDAD.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Sanidad.
a.2) Finalidad: Gestión y control de todo el historial clínico del personal de la Guardia Civil, en cumplimiento de lo previsto en los artículos 45 d), 49, 96.1 y 97 de la Ley 42/1999, de 25 de noviembre, de Régimen del Personal de la Guardia Civil.
a.3) Usos previstos: Administrativo, atención y gestión sanitaria, control del absentismo y epidemiológico.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal del Cuerpo y del Ministerio de Defensa destinados o adscritos a la Guardia Civil; personal dependiente del Ministerio del Interior (funcionarios civiles y personal laboral) que prestan servicios en el seno de la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Del propio interesado o su representante legal, mediante entrevistas y formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono.
Datos de características personales: Fecha de nacimiento, edad, sexo.
Datos de circunstancias sociales: Situación militar.
Datos académicos y profesionales: Formación, titulaciones, historial del estudiante, experiencia profesional e incorporación o integración en colegios o asociaciones profesionales.
Datos de detalle de empleo: Cuerpo/Escala, Categoría/Grado, puesto de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Juntas Médico Periciales del Ministerio de Defensa, en virtud de lo previsto en la Ley 42/1999, de 25 de noviembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Guardia Civil, calle Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Guardia Civil - Jefatura de Asistencia al Personal, calle Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

47. FICHERO: SEGPRIVA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SEGPRIVA.
a.2) Finalidad: Gestión y control de las competencias de la Guardia Civil en todos los aspectos relacionados con los Guardas Particulares de Campo en sus distintas especialidades, instructores de tiro de seguridad privada, acreditaciones para profesorado de Guardas Particulares de Campo y sus especialidades, procedimientos sancionadores en materia de seguridad privada y contratos de servicios en este mismo ámbito, así como aquellas materias relacionadas con la seguridad privada en las que intervenga o de las que participe la Guardia Civil.
a.3) Usos previstos: Administrativo y de investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Guardas particulares de campo y sus especialidades (guardas de caza y guardapescas marítimos) e instructores de tiro de seguridad privada. Cualquier persona que solicite participar en las pruebas de selección para Guardas Particulares de Campo y sus especialidades, instructores de tiro del personal de seguridad privada o acreditaciones para profesorado de Guardas Particulares de Campo y sus especialidades. Personas relacionadas con planes y actuaciones que se lleven a efecto en el sector de la seguridad privada en los que intervenga o participe la Guardia Civil.
b.2) Procedencia y procedimiento de recogida: Grabación de los datos por las unidades territoriales de la Guardia Civil, aportados por el propio interesado o su representante legal, y las publicaciones en el BOE, en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos especialmente protegidos: Salud.
Datos relativos a la comisión de infracciones penales o administrativas: Infracciones penales y administrativas.

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección postal, teléfono, dirección de correo electrónico y otros documentos identificativos.
Datos de características personales.
Datos académicos y profesionales.
Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Fuerzas y Cuerpos de Seguridad, a los Órganos Jurisdiccionales y al Ministerio Fiscal, en virtud de lo establecido en los artículos 3 y 45 de la Ley Orgánica 2/1986, de 13 de marzo, y de conformidad con los artículos 11.2.a) y d) y 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Unidades Especiales y de Reserva, C/ Guzmán el Bueno, 110, 28003 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

48. FICHERO: SOCORROS MUTUOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Socorros mutuos.
a.2) Finalidad: Control y gestión del cobro de cuotas a personal de la Guardia Civil pertenecientes a la Asociación de Socorros Mutuos de la Guardia Civil y pagos de derramas a sus beneficiarios.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal de la Guardia Civil en cualquier situación administrativa o retirado y los beneficiarios de las derramas.
b.2) Procedencia y procedimiento de recogida: Del propio interesado mediante la cumplimentación de formularios en soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, y dirección postal.
Datos de características personales.
Datos de circunstancias sociales.
Datos de detalle de empleo.
Datos económico-financieros y de seguros.
Datos de transacciones.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) - Jefatura de Personal, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

49. FICHERO: COSEIN (CONTROL DE SEGURIDAD DE INSTALACIONES).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: COSEIN (Control de Seguridad de Instalaciones).

a.2) Finalidad: Gestionar la seguridad y control de acceso a los acuartelamientos, bases, centros y edificios de la Guardia Civil o donde preste servicio de seguridad la Guardia Civil y realice el control de acceso, mediante la identificación de las personas y vehículos.

a.3) Usos previstos: Seguridad, control interno e investigación policial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que acceden a las distintas dependencias de los acuartelamientos, bases, centros y edificios de la Guardia Civil o donde preste servicio de seguridad la Guardia Civil y realice en control de acceso.

b.2) Procedencia y procedimiento de recogida: Del propio interesado mediante la grabación de los datos aportados por la persona que pretende acceder al acuartelamiento, base, centro o edificio.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, imagen, dirección postal, teléfono y vehículo del interesado y otros documentos identificativos.

Datos de características personales.

Datos de detalle de empleo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Fuerzas y Cuerpos de Seguridad para sus funciones de protección de la seguridad pública, conforme a lo establecido en el artículo 22.2 de la Ley Orgánica 15/1999, de 13 de diciembre, en cumplimiento de los principios de colaboración, mutuo auxilio y cooperación e información recíprocas que establece la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil), C/ Guzmán el Bueno, 110, 28003 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de la Policía y de la Guardia Civil (Ámbito Guardia Civil) – Jefatura de Unidades Especiales y Reserva, C/ Guzmán el Bueno, 110, 28003 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Secretaría General de Instituciones Penitenciarias

1. FICHERO: INSPECCIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Inspección.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias a los efectos de ejercicio de la actividad fiscalizadora e inspectora sobre los mismos.
a.3) Usos previstos: Soporte a las tareas de Inspección Penitenciaria (asignación de guardias, novedades de la guardia, carga y libro de atención al ciudadano, etc.).

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios de la Dirección General de Instituciones Penitenciarias. Internos dependientes de la Dirección General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, n.º Reg. Personal, NIS (número de identificación de interno).
Datos de detalle del empleo: Categoría, puestos de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: VINCULACIÓN FAMILIAR.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Vinculación familiar.
a.2) Finalidad: Tratamiento y gestión de resoluciones de traslado de internos en situación de presos preventivos, por vinculación familiar.
a.3) Usos previstos: Gestión de solicitudes de traslados de internos entre centros penitenciarios por vinculación familiar.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los internos de los Centros Penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias, las personas sometidas a cualquier pena y/o medida

alternativa al ingreso en prisión, así como, estrictamente en lo que respecta a los datos de situación familiar y dinámica familiar, los de las familias de todos los anteriores, y/o las personas con vinculación afectiva similar.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Se adquirirán determinados datos por traspaso automático de datos de los recabados en el Sistema de Información Penitenciaria.

Procedimiento de recogida: Formularios, encuestas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos de carácter identificativo: NIS (número de identificación de interno), nombre y apellidos de los internos o personas con penas y/o medidas alternativa al ingreso en prisión, así como datos de situación familiar y dinámica familiar, de las personas familiares de todos los anteriores, y/o las personas con vinculación afectiva similar.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

3. FICHERO: PAGOS CENTRALIZADOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Pagos centralizados.

a.2) Finalidad: Gestión y control del gasto por indemnizaciones de centros e instituciones penitenciarias. La Administración Penitenciaria indemnizarán a los particulares por la aplicación de actos legislativos de naturaleza no expropiatoria de derecho y que éstos no tengan el deber jurídico de soportar, cuando así se establezcan en los propios actos legislativos y en los términos que especifiquen dichos actos.

a.3) Usos previstos: Gestión centralizada de gastos de centros penitenciarios.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Beneficiarios de indemnizaciones.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, Administraciones Públicas con competencias en esta materia, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios, encuestas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIF, nombre y apellidos.
Datos económicos de la indemnización.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Administración Tributaria, Entidades de crédito donde se realice el pago, Intervención General de la Administración del Estado y Tribunal de Cuentas.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

4. FICHERO: TALLAJE DE FUNCIONARIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Tallaje de funcionarios.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Gestión del vestuario asignado al personal de la Secretaría General de Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios y laborales de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIF, nombre y apellidos.
Datos de características personales: sexo, características físicas o antropométricas.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevén comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, Calle Alcalá 38-40, 28014, Madrid
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

5. FICHERO: GESTIÓN CENTROS PENITENCIARIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión Centros Penitenciarios.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias. Gestión de las Comunicaciones, gestión de peculio, ficha del interno sobre datos penales y datos de incidentes regimentales, al amparo de lo establecido en el Reglamento Penitenciario, aprobado por el Real Decreto 190/1996, de 9 de febrero.
a.3) Usos previstos: Gestión de centros penitenciarios (comunicaciones, recuentos, peculio, objetos de valor, ficha del interno e incidentes regimentales).

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias, familiares y comunicantes de los primeros.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, otras Administraciones públicas con competencias en materia penitenciaria, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, nombre y apellidos, NIS (número de identificación de interno), marcas físicas, datos identificación de comunicantes.
Datos de características personales: estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, características físicas o antropométricas.
Datos penitenciarios: responsabilidades penales e incidentes regimentales, datos de comunicaciones familiares.
Datos económico-financieros: datos económicos de la cuenta de peculio del interno.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Secretaría de Estado de Seguridad del Ministerio de Interior, de cara al cumplimiento de las funciones previstas en los artículos 12 y 13 de la Ley Orgánica 2/1986, de 13 de marzo.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

6. FICHERO: GASTO EN DIETAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gasto en dietas.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias. Recoge los datos de dietas y asignaciones para gastos de viaje de aquellas cantidades que la

Administración destina a indemnizar al trabajador cuando este tiene que desplazarse fuera del Centro de Trabajo.

a.3) Usos previstos: Gestión del gasto en dietas y pagos al profesorado por formación.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios de la Secretaría General de Instituciones Penitenciarias. Profesores que realizan tareas docentes para la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, Administraciones Públicas con competencias en la materia, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios, encuestas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIF, nombre y apellidos.

Datos económicos de la dieta o de las asignaciones por formación.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Intervención General de la Administración del Estado, Tribunal de Cuentas, Agencia Estatal de Administración Tributaria y entidades financieras donde se pueda producir el pago.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

7. FICHERO: BADARAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: BADARAL.

a.2) Finalidad: Gestión de personal de la Secretaría General de Instituciones Penitenciarias, incluida la relativa al Plan de Pensiones de la Administración General del Estado.

a.3) Usos previstos: Gestión de personal funcionario y laboral.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios y laborales de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, Administraciones Públicas con competencias en materia de personal, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios, encuestas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, nombre y apellidos, n.º de registro de personal.

Datos de circunstancias sociales: Licencias, permisos y autorizaciones.

Datos académicos y profesionales: Formación, titulaciones.

Datos de detalle del empleo: Cuerpo/escala, categoría/grado, puestos de trabajo, historial del trabajador.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio de Administraciones Públicas, para el ejercicio de sus competencias en la misma materia, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre, a las Entidades gestora y depositaria y a la Comisión de Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 19 de la Ley 61/2003, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2004 y el Texto Refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre. Registro Central de Personal, Ministerio de Presidencia, Entidad Gestora, Entidad Depositaria y Comisión de Control del Plan de Pensiones de la Administración General del Estado.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

8. FICHERO: SISTEMA DE IDENTIFICACIÓN AUTOMÁTICA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Sistema de identificación Automática.

a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias. Permite la captura, consulta y comparación automática de huellas dactilares agrupadas por fichas decadactilares y de los datos asociados al movimiento de los internos en el Sistema Penitenciario en cumplimiento de los dos mandatos fundamentales que la Constitución encomienda a la Administración Penitenciaria: La reinserción de los recluidos y la retención y custodia de los detenidos, presos y penados.

a.3) Usos previstos: Gestión de determinados aspectos de internos en los centros penitenciarios (movimientos intermódulos, altas, bajas, salidas, permisos, incidencias, etcétera).

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, otros Administraciones Públicas con competencias en materia penitenciaria, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
Procedimiento de recogida: Formularios, encuestas, entrevistas, sistemas biométricos.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIS (número de identificación de interno), nombre y apellidos, huellas dactilares y responsabilidades penales.
Datos de características personales: movimientos intermódulos, datos penales y penitenciarios de altas, bajas, salidas, permisos, incidencias.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Gabinete de Estudios de Seguridad Interior (GESI) de la Secretaría de Estado de Seguridad y las que hayan de realizarse a las Administraciones Públicas, Administración de Justicia y Fuerzas y Cuerpos de Seguridad, para el ejercicio de sus competencias en la materia, conforme a lo previsto en artículo 32 de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

9. FICHERO: LIBRETA DE DIRECCIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Libreta de direcciones.
a.2) Finalidad: Otras finalidades.
a.3) Usos previstos: Libreta de direcciones personales de correo electrónico.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios y laborales de la Secretaría General de Instituciones Penitenciarias. Personal externo al servicio de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: nombre y apellidos, dirección electrónica.
Datos de detalle del empleo: puestos de trabajo.

c.2) Sistema de tratamiento: No automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

10. FICHERO: CONTROL HORARIO.

a.3) Usos previstos: Control horario en servicios centrales, Centros Penitenciarios y Centros de Inserción Social (incluidos Servicios de Gestión de Penas y Medidas Alternativas).

b.2) Procedencia y procedimiento de recogida:

Procedencia: El propio interesado.
Procedimiento de recogida: Formularios y medios electrónicos.
Soporte utilizado para la obtención: Soporte papel y digital.

c.1) Descripción de los datos:

– datos de carácter identificativos: NIF/NIE, nombre, apellidos, número de carnet profesional, huella y foto.
– datos de detalle del empleo: Categoría y puesto de trabajo.
– datos de características personales: Datos relativos al cumplimiento horario del colectivo indicado en el presente fichero.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. Calle Alcalá, 38-40. 28014 Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias. Calle Alcalá, 38-40. 28014 Madrid, Centros Penitenciarios y Centros de Inserción Social.
(http://www.institucionpenitenciaria.es/web/portal/centrosPenitenciarios/localizacion.html)

11. FICHERO: TERCEROS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Terceros.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Datos de terceras personas físicas o jurídicas proveedores o adjudicatarias de contratación pública de la Secretaría General de Instituciones Penitenciarias. Datos de profesores que imparten cursos para la Secretaría General de Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas o jurídicas proveedores o adjudicatarias de contratación pública. Personas físicas que dan cursos para la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios.
Soporte utilizado para la obtención: Soporte papel, informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, Nombre y apellidos, dirección postal, teléfono.
Datos económico-financieros y de seguros: Datos bancarios.
Datos de información comercial: Actividades y negocios.
Datos de transacciones: Bienes y servicios suministrados por el afectado, transacciones financieras.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Intervención General de la Administración del Estado, Tribunal de Cuentas, Agencia Estatal de Administración Tributaria y entidades financieras donde se pueda producir el pago.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

12. FICHERO: SANIT.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SANIT.
a.2) Finalidad: Fines de atención sanitaria, fines de gestión sanitaria, y fines epidemiológicos.
a.3) Usos previstos: Control sanitario de la población reclusa en centros penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Historia Médica. Administraciones Públicas Sanitarias, en los términos autorizados en la Ley 41/2002, de 14 de noviembre, reguladora de la Autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.
Procedimiento de recogida: Formularios e informes.
Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno), DNI, sexo, fecha de nacimiento y procedencia.

Datos de Laboratorio: Pruebas de VIH, hepatitis, tuberculosis y otros datos generales de laboratorio.

Factores de riesgo de enfermedad: Conducta sexual, uso de drogas inyectadas y otros factores de riesgo.

Datos de prevención y tratamiento de enfermedades: Vacunaciones, tratamientos y otros datos médicos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, todo ello de conformidad con lo establecido en la Ley 41/2002, de 14 de noviembre, reguladora de la Autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica, y los artículos 7.3, 7.6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

13. FICHERO: ESTADÍSTICA SANITARIA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Estadística sanitaria.

a.2) Finalidad: Fines epidemiológicos y de gestión sanitaria.

a.3) Usos previstos: Registro de datos numéricos de atención sanitaria y registro individual de los ingresos hospitalarios entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Historia Médica. Administraciones Públicas Sanitarias, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, reguladora de la Autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica y el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos.
Datos del ingreso hospitalario: Diagnóstico, hospital y fecha de ingreso y alta hospitalaria.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica, y los artículos 7.3, 7.6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

14. FICHERO: FALLECIMIENTOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Fallecimientos.
a.2) Finalidad: Fines epidemiológicos.
a.3) Usos previstos: Registro de los fallecimientos entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Dirección General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: Historia Médica. Administraciones Públicas Sanitarias y Administración de Justicia, de conformidad con lo establecido en el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.
Procedimiento de recogida: Formularios de encuesta epidemiológica.
Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, sexo, fecha de nacimiento, edad, datos penitenciarios, y fecha de fallecimiento.
Datos del fallecimiento: Lugar y naturaleza del fallecimiento, causas del fallecimiento.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y

obligaciones en materia de información y documentación clínica, y los artículos 7.3, 7.6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

15. FICHERO: REGISTRO 196.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro 196.

a.2) Finalidad: Fines de gestión sanitaria. Gestión y control de centros e instituciones penitenciarias.

a.3) Usos previstos: Registro de las solicitudes de libertad condicional en aplicación del artículo 196 del Reglamento Penitenciario por enfermedad grave o incurable entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: Historia Médica, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica y en los artículos 7.3 y 7.6 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno).

Datos de la enfermedad que motiva la solicitud: Diagnóstico y fecha.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica. Órganos judiciales competentes para la resolución acerca de la puesta en libertad del interno, siempre que sea preciso, Juzgados y Tribunales.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.:

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

16. FICHERO: HOSPITAL PSIQUIÁTRICO DE SEVILLA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Hospital Psiquiátrico de Sevilla.

a.2) Finalidad: Fines de gestión sanitaria.

a.3) Usos previstos: Registro de los ingresos en el hospital psiquiátrico penitenciario de Sevilla.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: Historia Médica, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica. Administración de Justicia.

Procedimiento de recogida: Formularios.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno), domicilio, datos penales y judiciales.

Datos del ingreso: Diagnóstico y fecha de ingreso y de fin del internamiento.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

17. FICHERO: HOSPITAL PSIQUIÁTRICO DE ALICANTE.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Hospital Psiquiátrico de Alicante.
a.2) Finalidad: Fines de gestión sanitaria.
a.3) Usos previstos: Registro de los ingresos en el hospital psiquiátrico penitenciario de Sevilla.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: Historia Médica, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica. Administración de Justicia.
Procedimiento de recogida: Formularios.
Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno), domicilio, datos penales y judiciales.
Datos del ingreso: Diagnóstico y fecha de ingreso y de fin del internamiento.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

18. FICHERO: CUSXING.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Cusxing.
a.2) Finalidad: Fines de gestión sanitaria.
a.3) Usos previstos: Registro de los ingresos hospitalarios en hospitales de la Comunidad de Madrid de la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: Historia Médica. Administraciones Públicas Sanitarias, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.
Procedimiento de recogida: Formularios e informes médicos.
Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno), sexo, fecha de nacimiento, y prisión.
Datos del ingreso hospitalario: Diagnóstico, hospital y fechas de ingreso y alta.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

19. FICHERO: MARXENF.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Marxenf.
a.2) Finalidad: Fines de gestión sanitaria.
a.3) Usos previstos: Registro de las consultas hospitalarias en hospitales de la Comunidad de Madrid de la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:
Procedencia de los datos: Historia Médica. Administraciones Públicas Sanitarias, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, básica reguladora de la

autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.

Procedimiento de recogida: Formularios e informes médicos.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, y prisión.

Datos de la consulta hospitalaria: Hospital, servicio, prueba solicitada, y fecha de consulta.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se ajustará a lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

20. FICHERO: TBC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: TBC.

a.2) Finalidad: Fines epidemiológicos.

a.3) Usos previstos: Registro de los casos de tuberculosis diagnosticados entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Historia Médica. Administraciones Públicas Sanitarias, en los términos autorizados por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica y los artículo 7.3 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios de encuesta epidemiológica.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno), sexo, fecha de nacimiento, nacionalidad, y fecha de ingreso en prisión.
Factores de riesgo y protectores: Infección VIH, uso de drogas inyectadas, y otros factores de riesgo. Antecedentes vacunales y de tratamientos previos.
Datos de la enfermedad: Fecha, clínica y localización.
Datos de laboratorio: Radiología y Bacteriología.
Datos de tratamiento: Fecha de inicio y fármacos.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, todo ello de conformidad con lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica y el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

21. FICHERO: HEPC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: HEPC.
a.2) Finalidad: Fines epidemiológicos.
a.3) Usos previstos: Registro de las seroconversiones a la Hepatitis C entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Historia Médica, de conformidad con lo establecido en el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.
Procedimiento de recogida: Formularios de encuesta epidemiológica.
Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, sexo, fecha de nacimiento, fecha de ingreso en prisión.

Factores de riesgo: Conducta sexual, uso de drogas inyectadas, y otros factores de riesgo.

Datos de Laboratorio: Pruebas diagnósticas hepatitis C, prueba VIH y otros datos de laboratorio.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, al amparo de lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, y de derechos y obligaciones en materia de información y documentación clínica y del artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

22. FICHERO: EMS 2000I. SISTEMA DE MONITORIZACIÓN ELECTRÓNICA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: EMS 2000I. Sistema de monitorización electrónica.

a.2) Finalidad: Gestión y control de la monitorización por Medios Telemáticos.

a.3) Usos previstos: Monitorización y control remotos de presencia de los internos en tercer grado (u otra situación susceptible de ser controlada de modo remoto) designados por la Secretaría General de Instituciones Penitenciarias de acuerdo con sus programas de intervención.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Condenados a penas y medidas penales dependientes de la Secretaría General de Instituciones Penitenciarias. Funcionarios responsables de los programas de intervención.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Administraciones Públicas, al amparo de lo establecido en la Ley Orgánica 1/1979, de 26 de septiembre, General penitenciaria.

Procedimiento de recogida: Formularios, encuestas o entrevistas.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Números de DNI e internos de identificación en el sistema penitenciario, nombre y apellidos, Fecha de nacimiento, sexo.

Datos sobre características personales: Direcciones completas, lugar de destino dentro de la institución, teléfonos de su residencia, trabajo o localización.

Datos de infracciones: Infracciones penales, de conformidad con lo establecido en el artículo 7.1 del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario.

Datos sobre el seguimiento del programa de intervención: los derivados de la monitorización de la presencia/ausencia del interno en los lugares acordados.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Las que haya de realizarse a otras Administraciones Públicas para el ejercicio de sus competencias en la materia, en los términos permitidos por el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014, Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

23. FICHERO: EL CONTROL DE ACCESO Y VIGILANCIA DEL EDIFICIO SEDE DE LA SECRETARÍA GENERAL DE INSTITUCIONES PENITENCIARIAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: El control de acceso y vigilancia del edificio sede de la Secretaría General de Instituciones Penitenciarias.

a.2) Finalidad: Registro de imágenes obtenidas de las grabaciones efectuadas para el control y vigilancia a la hora de acceder al edificio sede de la Secretaría General de Instituciones Penitenciarias.

a.3) Usos previstos: Video vigilancia y seguridad.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que accedan al edificio.

b.2) Procedencia y procedimiento de recogida: Las imágenes son captadas y grabadas por las cámaras y videocámaras de seguridad instaladas en el edificio sede de la Secretaría General de Instituciones Penitenciarias. La encargada del tratamiento de las imágenes captadas será la empresa de seguridad que en cada momento preste servicios de vigilancia en la Secretaría General de Instituciones Penitenciarias, mediante condición prevista en contrato.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Al margen de que en principio puedan recogerse la totalidad de las imágenes obtenidas a través de los sistemas de video vigilancia captadas por las cámaras de seguridad instaladas en el edificio, únicamente se guardarán las imágenes de personas y colectivos sobre las que se inicie algún procedimiento sancionador penal, administrativo o disciplinario, así como del espacio en que se han obtenido y, en su caso, los datos referentes a la identidad de las personas o colectivos a quienes correspondan las imágenes (nombre, apellidos, edad, Documento Nacional de Identidad, domicilio, etcétera).

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Fuerzas y Cuerpos de Seguridad del Estado, de cara al

cumplimiento de las funciones previstas en los artículos 12 y 13 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28004 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

24. FICHERO: HISTORIAS CLÍNICAS EN CENTROS PENITENCIARIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Historias clínicas en Centros Penitenciarios.

a.2) Finalidad: Archivo de datos, valoraciones e informaciones sobre la situación y seguimiento de la salud de la población reclusa en los Centros Penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias.

a.3) Usos previstos: Control y seguimiento sanitario de la población reclusa en los Centros Penitenciarios.

a.4) Fines: Atención sanitaria, epidemiológicos y médico-legales.

b) Origen de los datos:

b.1) Colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos: Personas internas en los centros penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia: El propio interesado. Administraciones Públicas Sanitarias en los términos autorizados en la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

b.3) Procedimiento de recogida: Digitalización y tratamiento informatizado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, NIS (número de identificación del interno), sexo, fecha de nacimiento y procedencia.

Datos de Laboratorio: Pruebas de VIH, hepatitis, tuberculosis, y otros datos generales de laboratorio. Factores de riesgo de enfermedad: Antecedentes personales y familiares, conducta sexual, uso de drogas, y otros factores de riesgo.

Datos de prevención, diagnóstico y tratamiento de enfermedades: Exploración y pruebas médicas, diagnósticos, tratamientos, y otros datos médicos y de enfermería.

Datos médico-legales: Lesiones, intoxicaciones, salud mental, invalidez física o psíquica, y otros informes judiciales con datos médico-legales.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias realizar a otras Administraciones Públicas Sanitarias para la atención sanitaria de las personas o para solucionar una urgencia que requiera acceder a un fichero y las necesarias para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, todo ello de conformidad con lo establecido en la Ley 41/2002, de 14 de noviembre, y en los artículos 7.3, 7.6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

25. FICHERO: GESTIÓN DE PENAS DE TRABAJOS EN BENEFICIO DE LA COMUNIDAD (TBCS).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión de penas de trabajos en beneficio de la comunidad (TBCS).

a.2) Finalidad: Archivo de datos penales y de identificación de los penados a la pena de trabajo en beneficio de la comunidad dependientes de la Secretaría General de Instituciones Penitenciarias, que posibiliten la gestión y cumplimiento de la misma.

a.3) Usos previstos: Control y seguimiento de este tipo de población desde los Servicios de Gestión de Penas y Medidas Alternativas.

a.4) Fines: Control, verificación y seguimiento del cumplimiento de las penas de trabajo en beneficio de la comunidad, así como del resto de previsiones legales contempladas en la legislación vigente en el ámbito de las penas y medidas alternativas a la prisión.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas condenadas a penas de trabajo en beneficio de la comunidad dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia: El propio interesado. Tribunales Sentenciadores, Juzgados de lo Penal, Juzgados de Ejecutorias, Juzgados de Vigilancia Penitenciaria y resto de Autoridades Judiciales.

b.3) Procedimiento de recogida de los datos: Mandamientos de Ejecución Penal, Testimonios de Sentencias, Autos judiciales, entrevistas con el propio interesado.

b.4) Soporte utilizado para la obtención: Soporte papel.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, domicilio a efectos de notificaciones, DNI/NIE, número de la Seguridad Social, sexo, fecha de nacimiento y procedencia.

Otros datos de interés: Situaciones de invalidez física o psíquica, situaciones sociofamiliares o laborales que limiten o condicionen la realización del trabajo en beneficio de la comunidad. Datos de la infracción o delito cometido y datos de la condena.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias realizar a las Autoridades Judiciales, así como para el tratamiento estadístico de la información, en este caso bajo la protección y amparo del secreto estadístico, y a las entidades en que los penados presten sus servicios, con conformidad con lo dispuesto en el artículo 11.2 c) de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Servicios de Gestión de Penas y Medidas Alternativas, dependientes de la Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

26. FICHERO: LIBRO DE SERVICIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Libro de servicios.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Gestión servicios funcionarios y laborales en centros penitenciarios (Relación por número de seguridad de los funcionarios y laborales y servicios asignados a los mismos).

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:
b.1) Colectivo: Funcionarios y laborales de los centros penitenciarios dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, n.º reg. personal.
Datos de detalle del empleo: categoría, puestos de trabajo.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

27. FICHERO: PECULIO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Peculio.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Gestión de las cuentas de peculio de los internos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIS (número de identificación de interno), nombre y apellidos.
Datos económico-financieros: datos económicos de la cuenta de peculio del interno.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos: A entidades bancarias que tengan que realizar el pago; a Fuerzas y Cuerpos de Seguridad del Estado y Cuerpos de Policía de las Comunidades Autónomas para la prevención de un peligro real para la seguridad integral de las víctimas de violencia de género y para evitar futuros actos de violencia, en virtud del artículo 22.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

28. FICHERO: FIES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: FIES.
a.2) Finalidad: Gestión y control de internos en los ámbitos de régimen, tratamiento y seguridad.
a.3) Usos previstos: Control de internos de especial significación.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, Administraciones Públicas con competencia en la misma materia, de conformidad con lo previsto en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
Procedimiento de recogida: Formularios, encuestas o entrevistas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIS (número de identificación de interno), nombre y apellidos, dirección, marcas físicas.

Datos de características personales: datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, características físicas o antropométricas.

Datos de infracciones: infracciones penales, al amparo del artículo 15.2 de la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Secretaría de Estado de Seguridad del Ministerio del Interior, de cara al cumplimiento de las funciones previstas en los artículos 12 y 13 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

29. FICHERO: COMUNICACIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Comunicaciones.

a.2) Finalidad: Gestión de las comunicaciones y visitas de familiares, amigos autorizados, representantes legales, autoridades y profesionales realizadas a los internos de todos los Centros Penitenciarios, llevando el registro de las comunicaciones tanto ordinarias con familiares y amigos, como con representantes legales y visitas íntimas o familiares realizadas.

a.3) Usos previstos: Control de comunicaciones personales de los internos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias, familiares y comunicantes de los primeros.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, otras personas físicas distintas del afectado, al amparo de lo establecido en el artículo 51 de la Ley Orgánica 1/1979, General Penitenciaria y artículo 41 del Reglamento Penitenciario.

Procedimiento de recogida: Formularios, encuestas o entrevistas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, pasaporte o NIF, nombre y apellidos, NIS (número de identificación sistemática).

Datos de características personales: datos de familia (antropométricos y fotográficos, identificativos y residenciales).

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Secretaría de Estado de Seguridad del Ministerio del Interior, de cara al cumplimiento de las funciones previstas en los artículos 12 y 13 de la Ley Orgánica 2/1986, de 13 de marzo.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

30. FICHERO: SIP-INTERNOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SIP-Internos.

a.2) Finalidad: Gestión del ejercicio de las competencias legales de la Administración Penitenciaria en materia de ejecución penal y tratamiento penitenciario. Recoge toda la información penal y penitenciaria relativa a los trámites y resoluciones que configuran los expedientes de los internos preventivos y penados.

a.3) Usos previstos: Recogida, asentamiento y explotación de la información generada por la gestión identificada en el punto anterior.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, Administraciones Públicas con competencia en la misma materia, de conformidad con lo previsto en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios, encuestas o entrevistas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: NIS (número de identificación de interno), nombre y apellidos, dirección, marcas físicas.

Datos de características personales: datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, características físicas o antropométricas.

Datos de infracciones: infracciones penales y administrativas.

Datos penitenciarios: clasificación, permisos y actividades de tratamiento.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Otras Administraciones Públicas, conforme a lo establecido en el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre; Defensor del Pueblo o institución análoga de las Comunidades Autónomas, Ministerio Fiscal, Jueces o Tribunales, Fuerzas y Cuerpos de Seguridad del Estado, Embajadas y Consulados.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

31. FICHERO: CONTROL DE VISITAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Control de visitas.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Información de las personas que acceden a la sede central de la Secretaría General de Instituciones Penitenciarias. Control de acceso a las instalaciones de centros penitenciarios.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que acceden a la sede central de la Secretaría General de Instituciones Penitenciarias y a centros penitenciarios dependientes de ésta.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, nombre y apellidos.
Datos de detalle del empleo: categoría, puestos de trabajo.
Datos de información comercial: actividades o negocios.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

32. FICHERO: NEDAES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: NEDAES.
a.2) Finalidad: Gestión de nómina y de la aportación al Plan de Pensiones de la Administración General del Estado.

a.3) Usos previstos: Gestión de la nómina del personal al servicio de la Secretaría General de Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios y laborales de la Secretaría General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios.
Soporte utilizado para la obtención: Soporte papel, soporte informático.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI/NIF, nombre y apellidos, n.º SS/Mutualidad, N.º Registro Personal.
Datos de características personales: fecha de nacimiento.
Datos de detalle del empleo: cuerpo/escala, categoría/grado, puestos de trabajo.
Datos de detalles del empleo: datos no económicos de nómina.
Datos económico-financieros: ingresos, datos bancarios, datos deducciones impositivas/ impuestos.
Datos de afiliación sindical.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Administraciones Públicas para el ejercicio de competencias en la misma materia, al amparo de lo establecido en el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, a la Administración Tributaria al amparo de la Ley del Impuesto de la Renta de las Personas Físicas, a las Entidades gestora y depositaria y a la Comisión del Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 19 de la Ley 61/2003, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2004 y el Texto Refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre. Ministerio de Economía y Hacienda, Ministerio de Administraciones Públicas, Ministerio de Trabajo y Seguridad Social, Administración de Justicia, Sindicatos. Tesorería General de la Seguridad Social, MUFACE, Intervención General de la Administración del Estado, Tribunal de Cuentas y entidades financieras donde se abone la nómina.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

33. FICHERO: SOLICITA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Solicita.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Compensaciones por guerra civil.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas solicitantes de información penitenciaria a los efectos de presentar solicitudes de compensaciones por la Guerra Civil, en virtud de la Disposición Adicional Decimoctava (Indemnización por tiempo de prisión) de la Ley 4/1990, de 29 de junio, de Presupuestos Generales del Estado para 1990, la Orden EHA/2966/2007, de 11 de octubre, por la que se establecen ayudas para compensar la carga tributaria de las indemnizaciones percibidas del Estado o de las CC.AA., por privación de libertad derivadas de la Ley 46/1977, así como de la Ley 52/2007, de 26 de diciembre, por la que se reconocen y amplían derechos y se establecen medidas en favor de quienes padecieron persecución o violencia durante la guerra civil y la dictadura.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Los cónyuges viudos de los causantes.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: soporte papel/soporte informático.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre y apellidos, dirección, teléfono.
Datos de características personales: fecha de nacimiento, lugar de nacimiento.
Datos de circunstancias personales: historial en centros penitenciarios.
Datos económicos necesarios para el abono e la indemnización.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Intervención General de la Administración del Estado, Tribunal de Cuentas, Administración Tributaria y entidades financieras en las que se abone la indemnización.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

34. FICHERO: CASOSSIDA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: CASOSSIDA.

a.2) Finalidad: Fines epidemiológicos.

a.3) Usos previstos: Registro de los casos nuevos de SIDA diagnosticados entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Historia Médica. Administraciones Públicas Sanitarias al amparo de lo establecido en el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios de encuesta epidemiológica.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, sexo, fecha de nacimiento, edad, domicilio, país de origen, fecha fallecimiento.

Factores sociales y de riesgo: Conducta sexual, uso de drogas inyectadas, y otros factores de riesgo.

Datos de la enfermedad indicativa de SIDA: Enfermedad y fecha. Otras enfermedades asociadas.

Datos de Laboratorio: Prueba VIH y otros datos de laboratorio.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, al amparo de lo establecido en el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias. La gestión y custodia del historial clínico del paciente estarán bajo la responsabilidad del centro sanitario correspondiente o de los profesionales que en su caso desarrollen su actividad de manera individual.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

35. FICHERO: ENFERMEDADES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Enfermedades.

a.2) Finalidad: Fines epidemiológicos.

a.3) Usos previstos: Registro de los casos nuevos de enfermedades de declaración obligatoria según la legislación nacional y autonómica diagnosticadas entre la población reclusa en Instituciones Penitenciarias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Internos dependientes de la Secretaría General de Instituciones Penitenciarias.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado. Historia Médica. Administraciones Públicas Sanitarias, al amparo de lo establecido en el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios de encuesta epidemiológica.

Soporte utilizado para la obtención: Soporte papel y soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos personales: Nombre y apellidos, fecha nacimiento, edad, sexo, nacionalidad, NIS (número de identificación del interno).
Datos de la enfermedad declarada: Enfermedad y fecha. Factores de riesgo (VIH, uso de drogas inyectadas, otros).

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Aquéllas que sean necesarias para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica, al amparo de lo establecido en el artículo 11.2.f de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

36. FICHERO: SEGURIDAD.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Seguridad.
a.2) Finalidad: Gestión y control de centros e instituciones penitenciarias.
a.3) Usos previstos: Apoyo a Coordinación de seguridad.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios y laborales, personal externo trabajando para la Dirección General de Instituciones Penitenciarias, personas con alguna relación con la Dirección General de Instituciones Penitenciarias.
b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado.
Procedimiento de recogida: Formularios, encuestas.
Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, nombre y apellidos, dirección.
Datos de detalles de empleo: empresa u organización a la que pertenece.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Otros Órganos del Ministerio del Interior y Fuerzas y Cuerpos de Seguridad.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá, 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

37. FICHERO: PERSONAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Personal.

a.2) Finalidad: Gestión de personal de la Secretaría General de Instituciones Penitenciarias, incluida la relativa al Plan de Pensiones de la Administración General del Estado.

a.3) Usos previstos: Gestión de personal funcionario y laboral.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Funcionarios y laborales de la Secretaría General de Instituciones Penitenciarias. Personas que participan oposiciones a los Cuerpos de Instituciones Penitenciarias y procesos de selección de personal.

b.2) Procedencia y procedimiento de recogida:

Procedencia de los datos: El propio interesado, Administraciones Públicas con competencias en materia de personal, en los términos permitidos por el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

Procedimiento de recogida: Formularios, encuestas.

Soporte utilizado para la obtención: Soporte papel; soporte informático/magnético.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: DNI, nombre y apellidos, n.º de registro de personal.

Datos de circunstancias sociales: licencias, permisos y autorizaciones.

Datos académicos y profesionales: formación, titulaciones.

Datos de detalle del empleo: cuerpo/escala, categoría/grado, puestos de trabajo, historial del trabajador.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A las Entidades gestora y depositaria y a la Comisión de Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 19 de la Ley 61/2003, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2004 y el Texto Refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, c/ Alcalá 38-40, 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

38. FICHERO: SISPE-A (SISTEMA DE INFORMACIÓN SOBRE PENAS ALTERNATIVAS).

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: SISPE-A (Sistema de información sobre penas alternativas).

a.2) Finalidad: Gestión Administrativa de las penas de trabajos en beneficio de la comunidad, y de las suspensiones y sustituciones de condenas de penas privativas de libertad, mediante la implantación del uso de nuevas tecnologías en los sistemas y protocolos de trabajo de los Servicios de Gestión de Penas y Medidas Alternativas dependientes de los Establecimientos Penitenciarios (Centros Penitenciarios y Centros de Inserción Social) de la Secretaría General de Instituciones Penitenciarias.

a.3) Usos previstos: Gestión administrativa de las penas de trabajo en beneficio de la comunidad y suspensiones y sustituciones de condena, así como la realización de programas de intervención asociados a las penas y medidas alternativas competencia de la Institución Penitenciaria.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretenda obtener los datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas sometidas a la pena de trabajo en beneficio de la comunidad, a suspensiones y sustituciones de condena de penas privativas de libertad, así como a la realización de programas de intervención asociados a las penas alternativas competencia de la Institución Penitenciaria.

b.2) Procedencia y procedimiento de recogida: Fichas de adscripción, declaraciones del interesado, documentales o telemáticas. Se adquirirán determinados datos por traspaso automático de datos de los recabados en el Sistema de Información Penitenciaria.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

– datos de carácter identificativo: DNI/NIF, nombre y apellidos, número de Afiliación a la Seguridad Social.

– datos de características personales: Situación familiar.

– datos académicos y profesionales: Estudios realizados, nivel de estudios alcanzados, formación específica, profesión.

– datos de infracciones penales y administrativas: causas penales.

– datos psico-socio-sanitarios: vinculados a la obligación penal de realización de programas terapéuticos de tipo sexual, drogodependencias, de tratamiento psicológico, o cualquier otro que así fuera decidido por la autoridad judicial competente. Ello responde fundamentalmente al tratamiento de datos en los casos de suspensiones y sustituciones de penas privativas de libertad y, en concreto, a la regla de conducta impuesta penalmente a los sometidos a estos programas de intervención, derivados de ciertas patologías/etiologías analizadas a la hora de enjuiciar el delito (artículos 80 a 88 del Código Penal).

– datos penitenciarios: situación de ingreso en centro penitenciario.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios:

– Tribunales, Jueces y Magistrados y Ministerio Fiscal en el ejercicio de las funciones que tienen atribuidas.

– Defensor del Pueblo o institución análoga de las Comunidades Autónomas que ejerzan competencias ejecutivas en materia penitenciaria.

– Administración General del Estado, de las Comunidades Autónomas, Local e Instituciones de carácter público competentes, respecto de los datos necesarios para el ejercicio de sus funciones (nombre, apellidos, documento de identidad y número de jornadas a realizar, o bien, en caso de realización de reglas de conducta, programa a realizar, así como los hechos probados de la sentencia), en cumplimiento de lo previsto en el artículo 49.1.ª del Código Penal, así como en el artículo 4.1 del Real Decreto 840/2011, de 17 de junio, por el que se establecen las circunstancias de ejecución de las penas de trabajo en beneficio de la comunidad y de localización permanente en centro penitenciario, de determinadas medidas de seguridad, así como de la suspensión de la ejecución de la penas privativas de libertad y sustitución de penas.

– Administraciones autonómicas que tengan transferidas competencias en materia penitenciaria.

– Servicios públicos responsables de la producción de estadísticas oficiales.

– Observatorio Estatal de Violencia sobre la Mujer, en cumplimiento de lo previsto en el artículo 25 del Real Decreto 840/2011, de 17 de junio.

– Delegación Especial del Gobierno contra la Violencia sobre la Mujer, en cumplimiento de lo previsto en el artículo 25 del Real Decreto 840/2011, de 17 de junio.

e) Transferencias internacionales de datos previstas a terceros países, con indicación en su caso, de los países de destino de los datos: en su caso, organismos y entidades internacionales con competencia en la materia, de conformidad con la Recomendación CM/Rec(2010)1 del Comité de Ministros a los Estados miembros sobre las reglas del Consejo de Europa relativas a la probation.

f) Órgano responsable del fichero: Secretaría General de Instituciones Penitenciarias, calle Alcalá, 38-40, 28014 Madrid.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General de Instituciones Penitenciarias, calle Alcalá 38–40. 28014 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

Las primeras medidas a adoptar, previas a la redacción del documento de Seguridad serán:

– Administración del Sistema: La Secretaría General de Instituciones Penitenciarias del Ministerio del Interior será el órgano administrativo encargado de administrar y mantener el entorno operativo y disponibilidad del sistema, teniendo la responsabilidad de la realización de las tareas necesarias que garanticen el correcto funcionamiento, la custodia y la seguridad del sistema, sin perjuicio de las atribuciones correspondientes a otros órganos de la administración con competencias asumidas en la materia y reguladas por convenios de cooperación tecnológica. Dichos convenios se ajustarán a las características del sistema y respetarán las garantías establecidas en el Real Decreto 1720/2007, de 21 de diciembre.

– Disponibilidad del Sistema: El sistema estará en funcionamiento durante las veinticuatro horas del día, todos los días del año, sin perjuicio de lo previsto en el siguiente párrafo. En ningún caso, la presentación telemática de escritos y documentos o la recepción de actos de comunicación por medios telemáticos implicarán la alteración de lo establecido en las leyes sobre el tiempo hábil para las actuaciones procesales, plazos y su cómputo, ni tampoco supondrá ningún trato discriminatorio en la tramitación y resolución de los procesos judiciales.

Cuando la ineludible realización de trabajos de mantenimiento u otras razones técnicas lo requieran, podrán planificarse paradas de los sistemas informáticos que afecten o imposibiliten de forma temporal el servicio de comunicaciones telemáticas. Estas paradas serán avisadas por el propio sistema informático con una antelación mínima de cuatro días, siempre que sea posible, indicando el tiempo estimado de indisponibilidad del servicio.

Cuando por cualquier causa el sistema no pudiera prestar el servicio en las condiciones establecidas se informará a los usuarios de las circunstancias de la imposibilidad a los

efectos de la eventual realización de actos procesales en forma no telemática y, en su caso, se expedirá, previa solicitud, justificante de la interrupción del servicio.

La custodia de la información gestionada a través del sistema corresponde al administrador del sistema, en las condiciones establecidas en el documento de Seguridad correspondiente que se elaborara posteriormente.

– Implantación del Sistema: La implantación del sistema se llevará a cabo de forma gradual en función de las posibilidades técnicas y presupuestarias de la Secretaría General de Instituciones Penitenciarias, respecto de aquellos Centros Penitenciarios de ella dependientes y tipos de procedimientos incluidos en cada fase del proceso de despliegue.

Del mismo modo será gradual la incorporación al sistema de los usuarios de los Servicios Sociales tanto internos como externos, de los Centros de Inserción Social.

– Perfiles de usuario: La línea general de atribución de Perfiles de Usuario de la aplicación SISPE se basará en la precisión de las características del usuario, sistematizada a través de la precisión de su perfil o conjunto de funciones profesionales por persona para el caso de los puestos unipersonales o grupo para el resto de puestos.

La forma de establecer perfiles se realizará por factores como:

1. Localización geográfica (Centro Penitenciario o Servicio Social Externo).
2. Funciones o actividad principal a realizar.
3. Recursos de información requeridos.
4. Procedimientos de actuación.

Así se han definido inicialmente los perfiles siguientes:

1. Subdirectores de Régimen y Tratamiento: el modo de acceso a datos exclusivamente en modo consulta a los datos de su Centro y los datos de los Servicios Sociales Externos adscritos.

2. Coordinadores Sociales: Modo de acceso a datos con capacidades de modificación de los datos de su Centro y funcionalidad completa incluido el permiso de realización exclusivo de traslados de Expedientes.

3. Trabajadores Sociales (en Centros o en Servicios Sociales): Modo de acceso a datos con capacidades de modificación de los datos de su Centro o Servicio Social con funcionalidad completa excepto permisos de realización de traslados de Expedientes.

4. Jefe de los Servicios Sociales Externos: Modo de acceso a datos con capacidades de modificación de los datos de su Servicio Social y funcionalidad completa con permisos de realización exclusivo de traslados de Expedientes.

5. Funcionarios de Apoyo, Directores de Programas y Funcionarios de Segunda Actividad: Modo de acceso a datos con capacidad de modificación pero exclusivamente en los procedimientos de recepción y escaneo de sentencias e informes y sin acceso al resto de funcionalidades mas que en modo consulta.

6. Funcionarios de Oficio de Gestión: Tienen acceso en modo modificación de datos pero solo en los procedimientos de Liberado Condicional y de Localización Permanente.

– Requisitos de acceso seguro al Sistema: El acceso al Sistema de información se realizara a través de páginas web, para lo cual el usuario del Sistema podrá utilizar un navegador Web que cumpla la especificación W3C HTML 4.01 o superior o a través de estándares abiertos y estándares internacionalmente reconocidos.

Adicionalmente, el Sistema establecerá comunicaciones seguras mediante servicios Web u otros mecanismos que la Secretaría General de Instituciones Penitenciarias determine, basados en dichos estándares, con el fin de posibilitar la operatividad con otros sistemas.

El protocolo para la comunicación entre el navegador Web y el sistema de información será HTTPS como versión segura del protocolo HTTP con un canal de comunicación seguro basado en SSL (Secure Socket Layers) (cifrado simétrico de, al menos, 128 bits utilizando encriptación SSL/TLS) entre el navegador del cliente y el servidor HTTP.

Para completar el nivel alto de seguridad se instalarán certificados de clave pública en los servidores. Estos certificados, para una mayor seguridad, serán firmados por una autoridad certificadora autorizada.

Se establecen los siguientes procedimientos de identificación y autenticación de usuarios:

– Procedimiento de identificación: La identificación de un usuario se deberá acreditar mediante una petición por escrito ante las Subdirecciones Generales de Medio Abierto y Medidas Alternativas o Coordinación Territorial, según el área funcional de que se trate, haciendo constar necesariamente el nombre y apellidos del usuario, su DNI, su destino (Centro Penitenciario o unidad si es usuario de Servicios Centrales) y una descripción breve del perfil de los datos que desea tratar. Esta petición deberá contar con el visto bueno del Director del Centro Penitenciario del usuario o Director de la Unidad de quien dependa. Las citadas Subdirecciones concederán, o no, la autorización de acceso a los datos de carácter personal que contiene el SISPE, para el desempeño de las funciones que se han encomendado al usuario, por un periodo de tiempo concreto mientras dicho usuario tenga que desempeñar estas funciones.

– Procedimiento de autenticación: Una vez concedido el acceso a los datos de un usuario, se le hará entrega en otro momento de un juego de dos contraseñas para proceder a autenticarse ante cada uno de los sistemas de información, es decir, la Red y la propia aplicación SISPE, para acceder a los datos cada vez que los necesite, según su perfil de acceso.

Se utilizará el Sistema estándar de Identificación y Autenticación de JBOSS en J2EE.

– Procedimiento de Almacenamiento de la Contraseña: Una vez concedido el acceso a los datos de un usuario y comunicado al usuario interesado el login y contraseña, se almacenará la contraseña dentro de la Aplicación para el proceso de validación. El registro de la contraseña, se realiza a través de la imagen hash del password, de manera que el administrador no pueda descifrarlo.

– Procedimiento de Auditoría: Para el cumplimiento de lo relativo al Control del Registro de Accesos a Datos Protegidos se habilitarán las siguientes medidas:

1. De cada intento de acceso se guardarán, como mínimo un «LOG de Registro de Accesos» donde se registra:

Quién accede.
Cuándo se accede.
Fichero de acceso.
Tipo acceso.
Si se autoriza el acceso.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Nombre	Comentario
RLPD_CODEXP	Expediente al que se ha accedido.
RLPD_DATACC	Tipo de datos al que se ha accedido:
	Corresponde al fichero protegido al que se accede.
	SO -datos sociales (salud).
	PE -datos penitenciarios (SIP).
	PR -datos judiciales (SIP y Medio abierto y Medidas Alternativas).
	DO -documento asociado al expediente.
RLPD_REGIST	Registro al que se ha accedido de la tabla que se ha especificado en el campo RLPD_DATACC.
RLPD_MODACC	Modo de acceso a los datos:
	M -modificación.
	C -consulta.

Los mecanismos que permiten este registro de accesos estarán bajo el control directo del responsable de seguridad competente, o Administrador Social sin que deban permitir la desactivación ni manipulación de los mismos.

El periodo mínimo de conservación de los datos registrados será de dos años.

Subsecretaría de Interior

1. FICHERO: GESTIÓN DE LOS RECURSOS HUMANOS DEL DEPARTAMENTO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Gestión de los recursos humanos del Departamento.
a.2) Finalidad: Gestión de personal, incluida la relativa al Plan de Pensiones de la Administración General del Estado.
a.3) Usos previstos: Administrativos, derivados de los trámites necesarios en materia de personal que corresponden a las funciones de la Subdirección General de Personal, Costes y Planificación de Recursos Humanos e Inspección.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal funcionario y laboral del Departamento.
b.2) Procedencia y procedimiento de recogida: Del fichero de datos generales del Ministerio de Política Territorial y Administración Pública, de otras Unidades del Ministerio del Interior y de la información facilitada por el propio interesado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos personales: nombre, apellidos y DNI.
Datos identificativos: Dirección, teléfono, número de seguridad social/mutualidad, número de registro de personal y firma/huella.
Datos de circunstancias sociales: estado civil y número de hijos.
Datos del puesto de trabajo.
Datos académicos y profesionales: títulos, cursos, diplomas y otros de la misma naturaleza.
Cuantías de las ayudas sociales reconocidas a los empleados públicos.
Datos especialmente protegidos: datos sobre enfermedades relevantes a estos efectos, y en su caso, invalidez. Datos sobre afiliación sindical.
Datos relativos a la comisión de infracciones.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Unidades y Departamentos de la Administración del Estado, para el ejercicio de competencias en la misma materia, de conformidad con lo establecido en el artículo 21 de la Ley Orgánica 15/1999, de 13 de mayo, así como a las Entidades gestora y depositaria y a la Comisión de Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 22 de la Ley 2/2008, de 23 de diciembre, de Presupuestos Generales del Estado para el año 2009, y el Texto Refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por el Real Decreto Legislativo 1/2002, de 29 de noviembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Subdirección General de Personal, Costes y Planificación de Recursos Humanos e Inspección.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Personal, Costes y Planificación de Recursos Humanos e Inspección.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

2. FICHERO: QUEJAS Y SUGERENCIAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Quejas y sugerencias.

a.2) Finalidad: Recogida y tratamiento de datos incluidos en los formularios de quejas y sugerencias existentes en las distintas Unidades dependientes de la Subsecretaría del Interior, así como en aquellos otros documentos que sean remitidos por los ciudadanos, bien por correo postal o electrónico, o bien a través de Internet, en los términos previstos en el Capítulo IV del Real Decreto 951/2005, de 29 de julio.

a.3) Usos previstos: Seguimiento y control de los datos reflejados en los distintos documentos por parte de la Subdirección General de Personal, Costes y Planificación de Recursos Humanos e Inspección.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que han formulado quejas y sugerencias, tanto en el formulario de quejas y sugerencias como mediante escritos presentados por correo postal, correo electrónico o bien a través de Internet.

b.2) Procedencia y procedimiento de recogida: De los propios documentos presentados por los ciudadanos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Nombre, apellidos, domicilio, documento nacional de identidad del interesado, así como nombre y apellidos de los funcionarios afectados. Motivo de la queja o sugerencia formulada.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Órganos de la Administración en los supuestos en que así lo prevea una norma con rango de ley o cuando la queja o sugerencia se refiera a los mismos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Subdirección General de Personal, Costes y Planificación de Recursos Humanos e Inspección.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Personal, Costes y Planificación de Recursos Humanos e Inspección.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

3. FICHERO: NÓMINA DE PERSONAL DE LOS SERVICIOS CENTRALES DEL MINISTERIO DEL INTERIOR.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Nómina de personal de los servicios centrales del Ministerio del Interior.

a.2) Finalidad: Pago de haberes al personal en activo. Pago de la aportación al Plan de Pensiones de la Administración General del Estado.

a.3) Usos previstos: Los necesarios para la realización de funciones que en materia de retribuciones de personal en activo tenga encomendadas la Subdirección General de Gestión Económica y Patrimonial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal adscrito a los Servicios Centrales.

b.2) Procedencia y procedimiento de recogida: Mediante documentos aportados por las Unidades competentes o entregados directamente por los interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos identificativos: NIF/DNI, nombre y apellidos, número de Seguridad Social/ Mutualidad.
Datos económico-financieros: Datos bancarios, Datos de la nómina y del Plan de Pensiones.
Datos de empleo: Cuerpo/Escala, categoría/empleo/grado, puestos de trabajo.
Datos familiares: Situación familiar y número de hijos.
Datos de circunstancias sociales: En su caso, afiliación sindical.
Datos de salud: Minusvalías.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la Agencia Estatal de Administración Tributaria; a la Tesorería General de la Seguridad Social; a la Mutualidad de Funcionarios de la Administración Central (MUFACE); a la Mutualidad General Judicial (MUGEJU); Al Instituto Social de las Fuerzas Armadas (ISFAS); a las Mutualidades y Colegios de Huérfanos a los que voluntariamente coticen los funcionarios; a la Entidad Gestora y Depositaria del Plan de Pensiones; a la Comisión de Control del Plan de Pensiones de la Administración General del Estado; a los Sindicatos, respecto de los datos identificativos de los trabajadores a los que se les realiza descuento en nómina de la cuenta sindical correspondiente, e importe descontado; a las Entidades Bancarias; a la Intervención General de la Administración del Estado y al Tribunal de Cuentas.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Subdirección General de Gestión Económica y Patrimonial.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Gestión Económica y Patrimonial. Calle Amador de los Ríos, 7. 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: CONTROL DE ENTRADA Y SALIDA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Control de entrada y salida.
a.2) Finalidad: control, por razones de seguridad, de la entrada y salida de personal y visitantes en el Ministerio del Interior.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal del Departamento y visitantes al mismo.
b.2) Procedencia y procedimiento de recogida: Los aportados por los propios interesados (visitantes) o por las unidades competentes del Departamento.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: DNI/NIF; nombre y apellidos; datos relativos al cargo.
c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Oficialía Mayor.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Oficialía Mayor. Ministerio del Interior. Calle Amador de los Ríos, n.º 7, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

5. FICHERO: REGISTRO ELECTRÓNICO DEL MINISTERIO DEL INTERIOR.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro Electrónico del Ministerio del Interior.
a.2) Finalidad: Anotaciones registrales de los asientos electrónicos efectuados en el Registro Electrónico para, en su caso, poder consultar la información registral de sus asientos.
a.3) Usos previstos: Recepción y remisión de las solicitudes, los escritos y las comunicaciones y de su documentación complementaria a la persona, órgano o unidad destinataria de la misma. Así como para fines estadísticos y para responder a las consultas de los propios usuarios sobre el hecho registral.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas físicas o personas jurídicas en los términos establecidos en el articulo 10 del Real Decreto 1671/2009, de 6 de noviembre.
b.2) Procedencia y procedimiento de recogida: Por archivo de los datos introducidos en el momento de realizar el asiento.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre, apellidos, DNI/NIF/ pasaporte o documento identificativo, dirección postal y electrónica, teléfono y fax.
Datos relativos a la solicitud, escrito o comunicación presentados: fecha, hora y número de asiento registral, así como documentación anexa que aporte la persona física o jurídica que lo presente. No se incluirán datos especialmente protegidos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Transmisión de la información y documentación a la persona, órgano o unidad destinataria de la misma.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Subsecretaría.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Oficialía Mayor, C/ Amador de los Ríos, 7, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

Dirección General de Apoyo a Víctimas del Terrorismo

1. FICHERO: AYUDASIS «BASE DE DATOS DE AFECTADOS POR EL TERRORISMO».

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: AYUDASIS «Base de datos de afectados por el terrorismo».

a.2) Finalidad: Gestión de la información relativa a personas afectadas por actos de terrorismo con objeto de prestar una asistencia integral a dicho colectivo, desde el momento inmediato hasta el seguimiento posterior.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los afectados por un acto terrorista.

b.2) Procedencia y procedimiento de recogida: La información se recaba en un primer momento de los servicios policiales, sanitarios o asistenciales prestadores de la primera atención de emergencia y posteriormente de los propios interesados, de sus familiares y de los organismos que ejecuten actuaciones administrativas, sociales o judiciales en relación con los hechos causantes de los daños o con la reparación de sus consecuencias.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

1) Acto terrorista con el que está relacionada la persona afectada.

2) Autoría y seguimiento de las diligencias judiciales de la causa y de la ejecución de la sentencia recaída en la misma.

3) Filiación, nacionalidad, DNI u otro documento de identificación, profesión, estado civil, domicilio y teléfono del afectado principal y familiares allegados.

4) Datos de situación socio-económica y necesidades de atención personal.

5) Ayudas, prestaciones, condecoraciones o reconocimientos recibidos o en curso de las Administraciones Públicas, Fundaciones o Asociaciones de Víctimas que integran la red colaboradora con la Administración en materia asistencial.

6) Datos administrativos de gestión.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otros órganos de la Administración General del Estado o de otras Administraciones Públicas en el ejercicio de sus competencias en materia de asistencia a este colectivo, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Apoyo a Víctimas del Terrorismo.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Apoyo a Víctimas del Terrorismo; C/ Amador de los Ríos, n.º 8; 28071, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

2. FICHERO: ASISTER.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: ASISTER.
a.2) Finalidad: Gestión de información relativa a personas afectadas por el terrorismo para la tramitación de expedientes de ayudas y resarcimientos competencia del Ministerio del Interior al amparo de la legislación sobre ayudas a las víctimas del terrorismo.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Afectados por terrorismo.
b.2) Procedencia y procedimiento de recogida: La información se recaba personalmente de los propios interesados o sus familiares en expedientes de resarcimientos tramitados en su favor por el Ministerio del Interior, y a través de diligencias policiales y judiciales a estos efectos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Acto terrorista con el que está relacionada la persona afectada.
Filiación, nacionalidad, DNI u otro documento de identificación, profesión, estado civil, domicilio, teléfono, daños, ayudas solicitadas.
Datos administrativos relativos a lo solicitado.
Datos de salud.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otros órganos de la Administración General del Estado o de otras Administraciones Públicas en el ejercicio de sus competencias en materia de asistencia a este colectivo, al igual que a los órganos del Ministerio de Economía y Hacienda competentes en materia de fiscalización y pago de las obligaciones reconocidas a cargo de la Hacienda Pública, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Apoyo a Víctimas del Terrorismo.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Ayudas a Víctimas del Terrorismo y de Atención Ciudadana; C/ Amador de los Ríos, 8, 28071, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: PROSELEC.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: PROSELEC.

a.2) Finalidad: Resultados de los procesos selectivos en materia de personal del Ministerio de Interior.
a.3) Usos previstos: Informar a los interesados sobre su estado de participación y sus calificaciones en las diversas oposiciones y demás procesos selectivos de personal del Departamento.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Participantes en las oposiciones y demás procesos selectivos del Ministerio del Interior.
b.2) Procedencia y procedimiento de recogida: Los datos proceden de la propia solicitud formulada por el interesado y de los acuerdos y resoluciones que se adoptan en el curso del proceso selectivo.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Filiación (nombre y apellidos, DNI, fecha de nacimiento), circunstancias relativas a la participación en el proceso selectivo: número de opositor, calificaciones, admisión, causas de exclusión, citaciones, etc.
c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Apoyo a Víctimas del Terrorismo.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Ayudas a Víctimas del Terrorismo y de Atención Ciudadana; C/ Amador de los Ríos, 8, 28071, Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

Dirección General de Protección Civil y Emergencias

1. FICHERO: PERSONAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Personal.
a.2) Finalidad: Control interno de personal.
a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal de la Dirección General de Protección Civil.
b.2) Procedencia y procedimiento de recogida: Ficha de personal, con datos proporcionados por los propios interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos (nombre y apellidos, NIF, domicilio y teléfono), datos académicos (titulaciones, cursos e idiomas) y datos profesionales (cuerpo, puesto de trabajo y nivel).
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

2. FICHERO: CURSOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Cursos.
a.2) Finalidad: Contener los datos relevantes sobre la formación de personal.
a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Alumnos y profesores.
b.2) Procedencia y procedimiento de recogida: Instancia cumplimientada por los interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: datos identificativos (nombre, apellidos, NIF domicilio), datos académicos (titulaciones), datos profesionales (cuerpo o categoría profesional, puesto de trabajo).
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

3. FICHERO: SUBVENCIONES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Subvenciones.
a.2) Finalidad: Control y gestión subvenciones concedidas.
a.3) Usos previstos: Administrativo y de gestión.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Solicitantes de subvenciones.
b.2) Procedencia y procedimiento de recogida: Instancia cumplimentada por los propios interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos (nombre y apellidos NIF, domicilio en el supuesto de particulares, datos económicos (importe de la subvención concedida).
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Al Ministerio de Hacienda para el ejercicio de sus competencias en materia de gasto público.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

4. FICHERO: CATÁLOGO DE RECURSOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Catálogo de Recursos.
a.2) Finalidad: Relación de recursos movilizables en caso de emergencia.
a.3) Usos previstos: Disposición de recursos movilizables en caso de emergencia.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Cualquier ciudadano o empresa con recursos movilizables.
b.2) Procedencia y procedimiento de recogida: Formulario cumplimentado por los propios interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos identificativos de la persona de contacto (nombre dirección y teléfono).
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Protección Civil y Emergencias
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Protección Civil y Emergencias.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

Dirección General de Tráfico

1. FICHERO: REGISTRO DE VEHÍCULOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro de vehículos.
a.2) Finalidad: Gestión de las competencias propias. Información a interesados legítimos y terceros interesados. Elaboración de estadísticas internas y públicas. Anotación a instancia de otros Órganos, Registros y Entidades, con trascendencia para este registro de vehículos.
a.3) Usos previstos: Registro de vehículos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares de vehículos, Registro de Bienes Muebles, Consorcio de Compensación de Seguros, Ministerio de Industria, Turismo y Comercio, Concesionarios de vehículos, Estaciones de Inspección Técnica de Vehículos, Fabricantes de Automóviles, Camiones y Autobuses y Registro Oficial de Maquinaria Agrícola.
b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los interesados, transmisión electrónica y fuentes accesibles al público.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de vehículos, con su identificación, matrícula y número de bastidor, datos de titularidad (nombre, apellidos y DNI o NIE), domicilio, Dirección Electrónica Vial (DEV), datos técnicos, trámites, inspecciones técnicas, precintos, limitaciones y cargas, eventuales poseedores, conductor habitual y arrendatario a largo plazo y seguro.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Se trata de un registro público, de conformidad con lo establecido en el artículo 2 del Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre. Se prevén cesiones a la Administración Tributaria, Administración de la Seguridad Social, Servicio Catalán de Tráfico y Dirección de Tráfico del Gobierno Vasco, Ayuntamientos, Diputaciones y Cabildos, Fuerzas y Cuerpos de Seguridad, Juzgados, Ministerio de Fomento, Ministerio de Industria, Turismo y Comercio y Consejerías de Industria de Comunidades Autónomas, Estaciones de Inspección Técnica de Vehículos, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Tráfico.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071-Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

2. FICHERO: REGISTRO DE CONDUCTORES E INFRACTORES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro de conductores e infractores.
a.2) Finalidad: Registro de conductores e infractores en materia de tráfico.
a.3) Usos previstos: Gestión de las competencias propias previstas en el Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 339/1990, de 2 de marzo, relacionadas con las autorizaciones administrativas para conducir y con el ejercicio de la potestad sancionadora.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Solicitantes y titulares de permisos o licencias de conducción. Otras personas físicas que, no siendo titulares de las mencionadas autorizaciones administrativas en España, sean condenados por sentencia firme a la privación del derecho a conducir o sean sancionados por resolución firme por la comisión de infracciones graves o muy graves contempladas en la normativa de seguridad vial.

b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los interesados y transmisiones electrónicas; Transmisión por las propias unidades del organismo o por otras Administraciones con competencia sancionadora en materia de tráfico, al amparo de lo establecido en el artículo 93 del Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto Legislativo 339/1990, de 2 de marzo.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: al amparo de lo establecido en el artículo 76 y siguientes del Real Decreto 818/2009, de 8 de mayo, el que se aprueba el Reglamento General de Conductores, así como en el artículo 93 del Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, contiene datos de solicitantes y titulares de permisos y licencias de conducción: nombre y apellidos, DNI o NIE, fecha de nacimiento, sexo, clases de permisos y licencias de conducción de las que sea titular e historial, condiciones restrictivas, incidencias denegatorias o informativas, suspensiones de permisos, dirección postal, Dirección electrónica Vial (DEV), crédito de puntos y otras circunstancias de interés, así como datos de sanciones firmes graves y muy graves por infracciones a la Ley de Seguridad Vial impuestas por los Jefes Provinciales y Locales de Tráfico, el Servicio Catalán de Tráfico, la Dirección de Tráfico del Gobierno Vasco y los Alcaldes, con identificación, al menos, del expediente, datos del infractor (DNI o NIE, nombre y apellidos, fecha de nacimiento), fecha de la infracción, precepto infringido, calificación de la sanción, autoridad sancionadora, sanción impuesta, fecha de la resolución sancionadora y de firmeza de la sanción.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Servicio Catalán de Tráfico, Dirección de Tráfico del Gobierno Vasco y Ayuntamientos, en ejercicio de competencias en la misma materia al amparo de lo establecido en el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071-Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: RECURSOS HUMANOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Recursos humanos.

a.2) Finalidad: Gestión de Recursos Humanos y de las retribuciones, incluyendo las cotizaciones a los Regímenes de la Seguridad Social y retenciones de IRPF, las actuaciones de acción social a favor del personal, cursos de formación, provisión de personal laboral y

funcionario, así como la gestión del Plan de Pensiones de la Administración General del Estado.

a.3) Usos previstos: Administrativo y estadístico.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Empleados públicos, incluyendo beneficiarios del programa de acción social y del Plan de Pensiones de la Administración General del Estado.

b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por el interesado, por el Registro Central de Personal y transmisiones electrónicas, en los términos autorizados al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene información requerida para la administración de personal del Organismo y la gestión de sus retribuciones, cotizaciones y retenciones: datos personales (nombre y apellidos, DNI, NIE, NRP, retribuciones percibidas, domicilio, historial administrativo (puestos ocupados, fechas de nombramiento y cese), cursos recibidos, titulaciones académicas, sexo, fecha y lugar de nacimiento; grupo profesional cuerpo o escala, convenio (personal laboral), tipo contrato, fecha contrato, antigüedad; situación administrativa, jornada y destino.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras Unidades con competencias en la misma materia, al amparo de lo establecido en el artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre, a las Entidades gestora y depositaria y a la Comisión de Control del Plan de Pensiones de la Administración General del Estado, de conformidad con el artículo 19 de la Ley 61/2003, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2004 y el Texto Refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, aprobado por Real Decreto Legislativo 1/2002, de 29 de noviembre, así como a la Administración Tributaria, a la Administración de la Seguridad Social y a MUFACE.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: Registro Nacional de Víctimas de Accidentes de Tráfico.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro Nacional de Víctimas de Accidentes de Tráfico.

a.2) Finalidad: Disponer de información necesaria para determinar las causas y circunstancias en que se han producido los accidentes de tráfico con víctimas acaecidos en todo el territorio nacional y sus consecuencias, de acuerdo con lo previsto en el artículo 95 del texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 339/1990, de 2 de marzo; para elaborar la estadística nacional de accidentes de tráfico con víctimas, de acuerdo con lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública; para calcular el coste social medio de los accidentes mortales y de los accidentes graves de tráfico, en cumplimiento de lo previsto en el Real Decreto 345/2011, de 11 de marzo, sobre gestión de la seguridad de

las infraestructuras viarias en la Red de Carreteras del Estado; y para evaluar las medidas adoptadas y elaborar programas de actuación.

a.3) Usos previstos: Estadístico y de investigación.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

b.1) Colectivo: Personas implicadas en accidentes de tráfico con víctimas.

b.2) Procedencia y procedimiento de recogida: Remisión por medios electrónicos o en soporte papel de los formularios cumplimentados por los agentes de la autoridad encargados de la vigilancia y el control del tráfico.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

c.1) Descripción de los datos: Contiene información sobre el accidente (lugar, fecha y hora y coordenadas geográficas); los vehículos implicados (matrícula, marca y modelo); las personas implicadas (NIF, NIE, tarjeta de residencia, pasaporte, nombre y apellidos, fecha de nacimiento, nacionalidad).

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando, en su caso, los destinatarios o categorías de destinatarios: Ministerio Fiscal, Jueces y Tribunales y otras administraciones públicas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, calle Josefa Valcárcel, 44, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

5. FICHERO: CENTROS DE MANIPULACIÓN DE PLACAS DE MATRÍCULA.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centros de manipulación de placas de matrícula.

a.2) Finalidad: Gestión de competencias propias en materia de autorizaciones, control e inspección, de centros autorizados de manipulación de placas de matrícula.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares de centros autorizados de manipulación de placas de matrícula.

b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por el interesado, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene información requerida para la gestión, control e inspección de los centros autorizados de manipulación de placas de matrícula: nombre, apellidos DNI o NIE del titular del centro, fecha de apertura, domicilio, datos de actividad.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Administración Tributaria, Administración de la Seguridad Social, Fuerzas y Cuerpos de Seguridad, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

6. FICHERO: CENTROS AUTORIZADOS DE TRATAMIENTO DE VEHÍCULOS AL FINAL DE SU VIDA ÚTIL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centros autorizados de tratamiento de vehículos al final de su vida útil.

a.2) Finalidad: Gestión de las bajas de los vehículos, entregados en los centros autorizados de tratamiento de vehículos al final de su vida útil, y gestión de las tasas por la anotación de las bajas en el Registro de Vehículos.

a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares de centros autorizados tratamiento de vehículos al final de su vida útil.

b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por el interesado, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene información requerida para la gestión de las bajas de los vehículos entregados en los centros autorizados de tratamiento de vehículos al final de su vida útil: nombre, apellidos DNI o NIE del titular del centro, fecha de apertura, domicilio, datos de actividad.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Administración Tributaria, Administración de la Seguridad Social, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

7. FICHERO: PREVENCIÓN DE RIESGOS LABORALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Prevención de riesgos laborales.

a.2) Finalidad: Gestión informática interna de la prevención de riesgos laborales de la Dirección General de Tráfico (gestión de los riesgos, incidentes, accidentes de trabajo y enfermedades profesionales, formación específica en prevención de riesgos laborales, higiene industrial y medicina del trabajo).

a.3) Usos previstos: Gestión administrativa de la información referente a la aptitud del empleado para el desempeño de su puesto de trabajo. Gestión de historias clínico-laborales y vigilancia de la salud laboral, asistencias médicas de los empleados públicos de la Dirección General de Tráfico y usuarios del Servicio de Prevención y Salud Laboral, a desarrollar por el personal sanitario.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Empleados públicos al servicio de la Dirección General de Tráfico y personal ajeno que requiera asistencia sanitaria.

b.2) Procedencia y procedimiento de recogida: Cuestionarios a cumplimentar por los interesados, así como fichas protocolizadas que elabora el personal técnico del Servicio de Prevención para la implementación de evaluaciones de riesgos, mediciones, reconocimientos médicos, voluntarios u obligatorios, y otras actuaciones técnicas que se precisen.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de identificación del personal al servicio de la Dirección General de Tráfico, datos de localización de los mismos y datos médicos (historias médico-laborales, asistencial y vigilancia de la salud laboral, reconocimientos médicos).

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la autoridad laboral, en los términos previstos en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales y su desarrollo reglamentario, así como a las autoridades judiciales, en cumplimiento de lo establecido en el artículo 16.3 de la Ley 41/2002, de 14 de noviembre, de Autonomía del Paciente.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

8. FICHERO: MAPA DE CONOCIMIENTO EN PREVENCIÓN DE RIESGOS LABORALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Mapa de conocimiento en prevención de riesgos laborales.

a.2) Finalidad: Proporcionar información sobre los empleados públicos de la Dirección General de Tráfico que poseen formación específica en materia de prevención de riesgos laborales. Relación actualizada de Delegados de Prevención y Representantes del Organismo de los Comités de Seguridad y Salud Laboral y Comité Intercentros de Seguridad y Salud de la Dirección General de Tráfico.

a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal al servicio de la Dirección General de Tráfico o al de otros Departamentos Ministeriales u Organismos públicos que hayan sido designados por los órganos competentes como Delegados de Prevención y Representantes de la Dirección General de Tráfico en los Comités de Seguridad y Salud Laboral y Comité Intercentros de Seguridad y Salud.

b.2) Procedencia y procedimiento de recogida: Certificaciones expedidas por el Servicio de Prevención o entidad que imparta los correspondientes cursos de formación. Presentación de titulaciones por los interesados. Notificaciones de las Juntas de Personal o Comités de Empresa, o, en defecto de las anteriores, actas de designación por la mayoría del personal en cada centro de trabajo que cuente con un Comité de Seguridad y Salud Laboral; en cuanto a los representantes de la Dirección General de Tráfico, a través de los nombramientos efectuados por el Ilmo. Director General de Tráfico.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de identificación y unidad de destino de los delegados de prevención y representantes en los Comités de Seguridad y Salud Laboral: nombre y apellidos, número de registro personal, relación laboral (personal funcionario o laboral), unidad de destino, puesto de trabajo, curso realizado, año de realización y, en su caso, la pertenencia al Comité de Seguridad y Salud Laboral de la provincia correspondiente o al Comité Intercentros de Seguridad y Salud en calidad de Delegado de Prevención o Representante de la Dirección General de Tráfico, fecha de nombramiento y fecha en que deja de ostentar tal condición.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Defensor del Pueblo o entidad autonómica equivalente, Ministerio Fiscal, Jueces y Tribunales, Tribunal de Cuentas o entidad autonómica equivalente, y aquellas otras previstas en el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

9. FICHERO: VÍCTIMAS DE ACCIDENTES LABORALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Víctimas de accidentes laborales.

a.2) Finalidad: Gestión interna de la prevención de riesgos laborales. Obtener la información necesaria que facilite la investigación de los accidentes de los empleados públicos de la Dirección General de Tráfico adscritos a los regímenes de Seguridad Social y MUFACE.

a.3) Usos previstos: Gestión administrativa de la información referida a los accidentes de trabajo, reservando al personal sanitario la gestión de los datos relativos a la salud de los accidentados.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Empleados públicos al servicio de la Dirección General de Tráfico adscritos a los regímenes de Seguridad Social y MUFACE.

b.2) Procedencia y procedimiento de recogida: Aportados por el propio interesado, a través del volcado de información incluida en el sistema informático DeltU, por el que se tramitan los partes de accidente de trabajo del personal adscrito a Seguridad Social y mediante del envío por correo electrónico, del modelo de la ficha de accidente de trabajo del personal adscrito a MUFACE recogida en el Protocolo para la Gestión de Partes de Accidente de Trabajo de la Dirección General de Tráfico, todo ello al amparo de la normativa de prevención de riesgos laborales.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos del accidentado, lugar del accidente, centro de trabajo en que ocurrió el accidente y su adscripción, fecha del accidente, fecha de la baja médica y otras circunstancias del accidente.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A la autoridad laboral, en los términos previstos en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales y su desarrollo reglamentario, así como a las autoridades judiciales, en cumplimiento de lo establecido en el artículo 16.3 de la Ley 41/2002, de 14 de noviembre, de Autonomía del Paciente.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico C/ Josefa Valcárcel, 28, 28071-Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

10. FICHERO: CONTROL HORARIO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Control horario.

a.2) Finalidad: Gestión de funcionarios y laborales respecto a jornadas, vacaciones, licencias, permisos, gestiones personales u oficiales.

a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal destinado en los Servicios Centrales e histórico de los que han estado.

b.2) Procedencia y procedimiento de recogida: Lectores de tarjetas de identificación con banda magnética (fichas), realizando el propio interesado el procedimiento de lectura de la misma.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos personales de apellidos, nombre, DNI, alta/baja, número tarjeta, numero funcionario, núm. Seguridad social, calle, distrito postal, ciudad, teléfono, vacaciones anuales, permisos presidencia, antigüedad, calendario que debe cumplir, acceso a control horario, unidad al que está adscrito, tabla incidencias, tabla de contadores y saldos.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A otras unidades con competencias en la materia.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071-Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

11. FICHERO: ESCALAFÓN TÉCNICOS DE TRÁFICO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Escalafón de la Escala Superior de tráfico.

a.2) Finalidad: Gestión de funcionarios pertenecientes a la Escala Superior de Técnicos de Tráfico. Elaboración de listados para la confección de los escalafones.

a.3) Usos previstos: Gestión administrativa.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personal perteneciente a la Escala Superior de Técnicos de Tráfico.

b.2) Procedencia y procedimiento de recogida: Aportados por el propio interesado a través de las correspondientes fichas. Importación de tablas de escalafones precedentes.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos personales de apellidos, nombre, DNI, fecha nacimiento, fecha de nombramiento, núm. orden proceso selectivo, puesto de destino, órgano de destino, nivel del puesto y provincia de destino.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071-Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

12. FICHERO: POSTES SOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Postes SOS.

a.2) Finalidad: Gestión de las competencias propias, ayuda y asistencia a los conductores y usuarios a través de los Postes SOS y sistemas similares con la misma finalidad. Estadísticas internas y publicas. Uso resultante de determinados acuerdos judiciales o requerimientos de autoridad policial.
a.3) Usos previstos: Administrativo.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que solicitan ayuda o información a través de los sistemas indicados.
b.2) Procedencia y procedimiento de recogida: Verbalmente de los propios interesados, impresos cumplimentados por los interesados, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de identificación de las personas que solicitan la ayuda (nombre y apellidos, DNI o NIE), tipo de ayuda, del vehículo para el que la solicitan en su caso, compañía de seguros y datos de la póliza.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Fuerzas y Cuerpos de Seguridad, Juzgados, Compañías de seguros.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Tráfico.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071-Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

13. FICHERO: AUTORIZACIONES COMPLEMENTARIAS Y ESPECIALES DE CIRCULACIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Autorizaciones complementarias y especiales de circulación.
a.2) Finalidad: Gestión de los procedimientos relacionados con autorizaciones complementarias y especiales de circulación. Estadísticas internas y publicas. Uso resultante de determinados acuerdos judiciales o requerimientos de autoridad policial o tributaria.
a.3) Usos previstos: Administrativos y estadísticos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares de vehículos, transportistas, empresas de transporte, personas que pretenden obtener una autorización para circular de alguno de estos tipos.
b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por el interesado, transmisión electrónica y fuentes accesibles al público.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de personas titulares de vehículos (nombre y apellidos, DNI o NIE), de los vehículos, y de la carga en su caso, así como itinerario previsto.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Comunidades autónomas, Ayuntamientos, Diputaciones y Cabildos, en virtud de lo dispuesto en el Reglamento General de Vehículos, aprobado por el Real Decreto 2822/1998, de 23 de diciembre, Juzgados, Administración Tributaria, Administración de la Seguridad Social, Fuerzas y Cuerpos de Seguridad y Ministerio de Fomento.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071-Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

14. FICHERO: DIVULGACIÓN DE LA INFORMACIÓN DEL OBSERVATORIO NACIONAL DE SEGURIDAD VIAL.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Divulgación de la información del Observatorio Nacional de Seguridad Vial.

a.2) Finalidad: Recogida de datos de profesionales y de particulares interesados en la Seguridad Vial.

a.3) Usos previstos: Gestión de receptores de información del Observatorio Nacional de Seguridad Vial.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Profesionales y particulares interesados en la seguridad vial.

b.2) Procedencia y procedimiento de recogida: Se recogen a través de la suscripción de los interesados en el formulario de recepción de publicaciones que, a tal efecto, se recoge en la página web de la Dirección General de Tráfico o en la forma prevista en el apartado segundo del artículo 14 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por el Real Decreto 1720/2007, de 21 diciembre.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre, apellidos, correo electrónico, dirección postal, teléfono fijo, móvil, fax.

Datos de detalles de empleo: Cargo, organismo, dirección postal, teléfono fijo, móvil, fax, dirección web de su organización.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

15. FICHERO: PERSONAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Personas.

a.2) Finalidad: Complementario de los Registros de conductores e infractores, de Vehículos, de profesionales de la enseñanza de la conducción, de profesionales de centros de reconocimiento de conductores y de centros de sensibilización y reeducación vial.

a.3) Usos previstos: Gestión de competencias propias. Estadísticas internas y públicas. Uso resultante de determinados acuerdos judiciales o requerimientos de autoridad policial o tributaria.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que se relacionen con el Organismo Autónomo Jefatura Central de Tráfico en asuntos referidos a las competencias previstas en el artículo 5 de la LSV.

b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los interesados, transmisión electrónica y fuentes accesibles al público.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos personales: nombre y apellidos, DNI o NIE, fecha de nacimiento, sexo, domicilio, Dirección electrónica Vial (DEV).

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Administración Tributaria, Administración de la Seguridad Social, Ayuntamientos, Diputaciones y Cabildos, Fuerzas y Cuerpos de Seguridad, Juzgados, Defensor del Pueblo, Ministerio Fiscal, Tribunales, Tribunal de Cuentas y otras Administraciones públicas para el ejercicio de competencias en la materia al amparo del artículo 21.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

16. FICHERO: CENTROS DE RECONOCIMIENTO DE CONDUCTORES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centros de reconocimiento de conductores.

a.2) Finalidad: Recogida de información sobre titulares, directores y personal facultativo de Centros de reconocimiento de conductores destinados a verificar las aptitudes psicofísicas de los conductores.

a.3) Usos previstos: Gestión de las competencias propias. Elaboración de estadísticas internas y públicas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares, directores y facultativos de los Centros de reconocimiento de conductores destinados a verificar las aptitudes psicofísicas de los conductores.
b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los propios interesados, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Al amparo del artículo 25 del Real Decreto 170/2010, de 19 de febrero, por el que se aprueba el Reglamento de centros de reconocimiento destinados a verificar las aptitudes psicofísicas de los conductores, contiene información de los Centros, así como de sus titulares, directores y personal facultativo: nombre y apellidos, DNI o NIE, nacionalidad, domicilio del centro, historial de inspecciones realizadas al centro y sanciones que se les hubieran impuesto.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Administración Tributaria al amparo del Texto Refundido de la Ley sobre el Impuesto de las Personas Físicas, aprobado por Real Decreto Legislativo 3/2004, de 5 de marzo, Administración de la Seguridad Social al amparo del Texto Refundido de la Ley General de la Seguridad Social, aprobado por Real Decreto Legislativo 1/1994, de 20 de junio, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Tráfico.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico C/ Josefa Valcárcel, 28, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

17. FICHERO: CENTROS DE FORMACIÓN DE CONDUCTORES Y DE PROFESIONALES DE LA ENSEÑANZA DE LA CONDUCCIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Centros de formación de conductores y de profesionales de la enseñanza de la conducción.
a.2) Finalidad: Control de las escuelas particulares de conductores y de los profesionales de la enseñanza de la conducción.
a.3) Usos previstos: Gestión de las competencias propias. Elaboración de estadísticas internas y públicas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Profesores de formación vial, titulares, directores y profesores de Escuelas particulares de conductores.
b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los interesados, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Al amparo del artículo 41 del Real Decreto 818/2009, de 8 de mayo, por el que se aprueba el Reglamento General de Conductores y del artículo 50 del Real Decreto 1295/2003, de 17 de octubre, por el que se aprueba el Reglamento regulador de las Escuelas Particulares de Conductores, contiene información de las escuelas particulares de conductores, así como de sus titulares, directores y profesores: nombre y apellidos, DNI o NIE, fecha de nacimiento, domicilio del centro, historial, clases de autorizaciones administrativas para conducir.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Servicio Catalán de Tráfico y Dirección de Tráfico del Gobierno Vasco, Administración Tributaria, Administración de la Seguridad Social, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico C/ Josefa Valcárcel, 28, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

18. FICHERO: EXPEDIENTES DE SANCIÓN.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Expedientes de sanción.

a.2) Finalidad: Gestión del procedimiento sancionador en los expedientes tramitados por las Jefaturas Provinciales de Tráfico y por el Centro de Tratamiento de Denuncias Automatizadas, desde su inicio hasta su conclusión, incluyendo seguimiento e impulso de expedientes, emisión de notificaciones, envió a vía de apremio, etc.

a.3) Usos previstos: Elaboración de estadísticas internas y públicas. Gestión de las competencias propias.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Titulares de permisos o licencias de conducción y titulares de vehículos, que sean denunciados por la comisión de infracciones contempladas en la normativa de seguridad vial, cuya competencia corresponda a las Jefaturas Provinciales de Tráfico, al amparo del artículo 71 del Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. Otras personas físicas que, sin ser titulares de las indicadas autorizaciones, sean denunciadas por la comisión de infracciones a la normativa de seguridad vial.

b.2) Procedencia y procedimiento de recogida: Boletines de denuncia, cumplimentación de formularios electrónicos en ordenador de mano por los agentes de la Agrupación de Tráfico de la Guardia Civil, así como sistemas de grabación de voz y datos.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Datos relativos a la comisión de infracciones administrativas; número de expediente sancionador, con datos de la denuncia (hecho denunciado, precepto infringido, calificación, lugar, fecha y hora, etc.), de la sanción en su caso impuesta, del denunciado (nombre, apellidos, DNI o NIE, domicilio, etc.), del denunciante (número de identificación) y de las situaciones procesales transcurridas.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Administración Tributaria, Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

19. FICHERO: ADJUDICATARIOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Adjudicatarios.

a.2) Finalidad: Gestión del organismo relativa a los proveedores de bienes y servicios, incluyendo el control de pagos a estos y los efectos de carácter fiscal, cuando la transacción alcanza determinada cantidad.

a.3) Usos previstos: Elaboración de estadísticas internas y usos administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Proveedores de bienes y servicios.

b.2) Procedencia y procedimiento de recogida: Impresos y documentación aportada en las licitaciones por los propios interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene información requerida para la gestión económica de los contratos del Organismo con sus proveedores de bienes y servicios. Personas de contacto (nombre y apellidos, DNI o NIE, cargo en la empresa), datos económico-financieros.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas, Administración Tributaria, órganos competentes en materia de fiscalización del gasto y entidades en que se produzca el pago de los servicios.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071-Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

20. FICHERO: SUSCRIPTORES DE LA REVISTA DE TRÁFICO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Suscriptores de la revista de Tráfico.

a.2) Finalidad: Distribución por correo postal y electrónico de los números de la revista Tráfico editada por el Organismo.

a.3) Usos previstos: Usos administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Suscriptores de la revista Tráfico.
b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los interesados, transmisión electrónica.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene información requerida para la distribución por correo, postal y electrónico, de la revista Tráfico: Nombre y apellidos y dirección postal.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Defensor del Pueblo, Ministerio Fiscal, Tribunales y Tribunal de Cuentas, Administración Tributaria, órganos competentes en materia de fiscalización del gasto y entidades en que se produzca el pago de los servicios.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Tráfico.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 28, 28071-Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

21. FICHERO: VISITAS A LOS CENTROS DE GESTIÓN DE TRÁFICO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:
a.1) Identificación del fichero: Visitas a los centros de gestión de tráfico.
a.2) Finalidad: Gestión y control de la presencia de personas en los Centros ajenas al servicio.
a.3) Usos previstos: Elaboración de estadísticas y usos administrativos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Personas que visitan el Centro o que realizan trabajos, operaciones de mantenimiento, instalación, etc. sin ser funcionarios ni estar adscritos al servicio del centro.
b.2) Procedencia y procedimiento de recogida: Impresos cumplimentados por los propios interesados.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de identificación de la persona (nombre y apellidos, DNI o NIE), empresa u organización a la que pertenece y motivo de la visita.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Tráfico.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, C/ Josefa Valcárcel, 44, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

22. FICHERO: TABLÓN EDICTAL DE SANCIONES DE TRÁFICO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Tablón Edictal de Sanciones de Tráfico.
a.2) Finalidad: Gestionar el Tablón Edictal de Sanciones de Tráfico.
a.3) Usos previstos: Gestión administrativa de la publicación a través de edictos de las notificaciones a que dé lugar el procedimiento sancionador como consecuencia de la comisión de infracciones a la normativa sobre tráfico, circulación de vehículos a motor y seguridad vial, que no se hayan podido practicar en la Dirección Electrónica Vial o en el domicilio del interesado, con independencia de cuál sea la autoridad sancionadora competente.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Organismos emisores autorizados para solicitar la publicación a través de edictos en el Tablón Edictal de Sanciones de Tráfico de las notificaciones que no se hayan podido practicar en la Dirección Electrónica Vial o en el domicilio del interesado.
b.2) Procedencia y procedimiento de recogida: Aplicaciones informáticas establecidas al efecto.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de los organismos emisores autorizados para solicitar la publicación a través de edictos de las notificaciones: nombre, apellidos, DNI o NIE, clave pública de la firma electrónica; así como los datos de las personas a las que se notifica mediante los edictos: nombre, apellidos o denominación social, DNI, NIE o CIF.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Defensor del Pueblo, Ministerio Fiscal, Agencia Estatal de Administración Tributaria, Jueces y Tribunales.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se prevén.
f) Órgano responsable del fichero: Dirección General de Tráfico.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico,calle Josefa Valcárcel, 44, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

23. FICHERO: LISTA DE EXCLUIDOS DEL TABLÓN EDICTAL DE SANCIONES DE TRÁFICO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Lista de excluidos del Tablón Edictal de Sanciones de Tráfico.
a.2) Finalidad: Gestionar el servicio «lista de excluidos» del Tablón Edictal de Sanciones de Tráfico.
a.3) Usos previstos: Gestión administrativa de los datos personales de quienes soliciten el alta o la baja en el servicio «lista de excluidos» para impedir que puedan ser visualizados

por cualquier persona que acceda a los edictos publicados en el Tablón Edictal de Sanciones de Tráfico.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Aquéllas que soliciten el alta o la baja en el servicio lista de excluidos para que sus datos personales contenidos en los edictos publicados en el Tablón Edictal de Sanciones de Tráfico no puedan ser visualizados más que por ellos mismos y por las personas a las cuáles haya autorizado.
b.2) Procedencia y procedimiento de recogida: Aplicaciones informáticas establecidas al efecto.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Contiene datos de las personas que han solicitado el alta en el servicio «lista de excluidos»: nombre, apellidos, DNI o NIE, domicilio, clave pública de la firma electrónica.
c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: No se prevé comunicación de datos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se prevén.
f) Órgano responsable del fichero: Dirección General de Tráfico.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Tráfico, calle Josefa Valcárcel, 44, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

Dirección General de Política Interior

1. FICHERO: APÁTRIDAS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Apátridas.
a.2) Finalidad: Comprende los expedientes de solicitud del estatuto de apátrida.
a.3) Usos previstos: Gestión administrativa, identificación y control de los solicitantes y de los apátridas; estadísticas internas y públicas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Solicitantes del estatuto de apátrida y apátridas.
b.2) Procedencia y procedimiento de recogida: El propio interesado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos Especialmente Protegidos: Origen racial o étnico, datos relativos a la comisión de infracciones penales o administrativas.
Datos de Carácter Identificativo: Nombre y apellidos, alias, dirección, teléfono, firma/huella, imagen, pasaportes, otros documentos...

Datos de Características Personales: Estado civil, familia, fecha y lugar de nacimiento, nacionalidad, características físicas o antropométricas, sexo, lengua, ...
Datos de Circunstancias Sociales: Lugares de residencia, domicilios.
Datos Académicos y Profesionales.
Datos Económicos-Financieros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los órganos jurisdiccionales, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de enero.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Dirección General de Política Interior.
g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Asilo (Oficina de Asilo y Refugio), c/ Pradillo, 40, 28071 Madrid.
h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

2. FICHERO: DESPLAZADOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Desplazados.
a.2) Finalidad: Comprende los expedientes de protección temporal.
a.3) Usos previstos: Facilita la gestión administrativa y la identificación y control de los solicitantes de protección temporal y de los desplazados; estadísticas internas y públicas.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Solicitantes de protección temporal y desplazados.
b.2) Procedencia y procedimiento de recogida: El propio interesado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de Carácter Identificativo: Nombre y apellidos, alias, dirección, teléfono, firma/huella, imagen, voz, marcas físicas, pasaportes, otros documentos...
Datos de Características Personales: Estado civil, familia, fecha y lugar de nacimiento, nacionalidad, características físicas o antropométricas, sexo, lengua...
Datos de Circunstancias Sociales: Alojamiento, vivienda, situación militar, propiedades, posesiones, aficiones y estilo de vida, pertenencia a clubes, asociaciones...
Datos Académicos y Profesionales: Formación, titulaciones, expediente académico, experiencia profesional, pertenencia a asociaciones profesionales...
Datos Económicos-Financieros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios y transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A los órganos jurisdiccionales, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de enero;
Estados miembros de la Unión Europea excepto Dinamarca, Comisión europea y ACNUR (Directiva de 20 de julio de 2001, relativa a las normas mínimas para la concesión de protección temporal en caso de afluencia masiva de personas desplazadas y a medidas

de fomento de un esfuerzo equitativo entre los Estados miembros para acoger a dichas personas y asumir las consecuencias de su acogida -DOCE de 07.08.01- y Real Decreto 1325/2003, de 24 de octubre, sobre régimen de protección temporal en caso de afluencia masiva de personas desplazadas).

e) Órgano responsable del fichero: Dirección General de Política Interior.

f) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Asilo (Oficina de Asilo y Refugio), c/ Pradillo, 40, 28071 Madrid.

g) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

3. FICHERO: ASILO.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Asilo.

a.2) Finalidad: Comprende los expedientes de solicitud de protección internacional; facilita la determinación del Estado responsable de las solicitudes de protección internacional en los Estados miembros de la Unión Europea, Noruega, Islandia, Suiza y Liechtenstein; la gestión administrativa y la identificación y control de los solicitantes de protección internacional; estadísticas internas y públicas.

a.3) Usos previstos: Gestión administrativa y estadístico.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Solicitantes de protección internacional.

b.2) Procedencia y procedimiento de recogida: El propio interesado.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos Especialmente Protegidos: Ideología, afiliación sindical, religión o creencias, origen racial o étnico, grupo social, salud, vida sexual, datos relativos a la comisión de infracciones penales o administrativas. Incluidos en virtud de la Ley 12/2009, de 30 de octubre, reguladora del derecho de asilo y de la protección subsidiaria.

Datos de Carácter Identificativo: Nombre y apellidos, alias, dirección, teléfono, firma/ huella, imagen, voz, marcas físicas, pasaportes, otros documentos...

Datos de Características Personales: Estado civil, familia, fecha y lugar de nacimiento, nacionalidad, características físicas o antropométricas, sexo, lengua...

Datos de Circunstancias Sociales: Alojamiento, vivienda, situación militar, propiedades, posesiones, aficiones y estilo de vida, pertenencia a clubes, asociaciones...

Datos Académicos y Profesionales: Formación, titulaciones, expediente académico, experiencia profesional, pertenencia a asociaciones profesionales...

Datos Económicos-Financieros.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios y transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: A los órganos jurisdiccionales, de conformidad con lo establecido en el artículo 11.2.d) de la Ley Orgánica 15/1999, de 13 de enero.

ACNUR, en virtud de los artículos 34 y 35 de la Ley 12/2009, de 30 de octubre, reguladora del derecho de asilo y la protección subsidiaria.

Estados miembros de la Unión Europea, Noruega, Islandia, Suiza y Liechtenstein, al amparo del Reglamento CE 343/2003, de 18 de febrero, por el que se establecen los

criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país.

e) Órgano responsable del fichero: Dirección General de Política Interior.

f) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Asilo (Oficina de Asilo y Refugio), c/ Pradillo, 40, 28071 Madrid.

g) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

4. FICHERO: REGISTRO DE PARTIDOS POLÍTICOS.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro de Partidos Políticos.

a.2) Finalidad: Inscripción de los partidos políticos que así adquieren personalidad jurídica.

a.3) Usos previstos: Registro Público en el que se incluyen todos los partidos políticos legalmente constituidos en España.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Promotores de las formaciones políticas.

b.2) Procedencia y procedimiento de recogida: Se obtienen de la solicitud de inscripción suscrita por cualquiera de los promotores o fundadores del partido, y del acta notarial suscrita por todos los promotores.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: Base de datos relacional. Datos personales de identificación.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios y transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: Solicitudes de información: Por cualquier persona interesada. Solicitudes de certificaciones: Por cualquier persona interesada o por los representantes de los partidos políticos, en este caso se requiere escrito con los datos personales de identificación del solicitante de la certificación. Solicitudes de certificaciones por parte de las distintas Juntas Electorales. Todo ello, de conformidad con lo señalado en la Ley Orgánica 6/2002, de 27 de junio, de Partidos Políticos y la Ley Orgánica 5/1985, de 19 de junio, de Régimen Electoral General.

e) Órgano responsable del fichero: Dirección General de Política Interior.

f) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Política Interior, c/ Amador de los Ríos, n.º 7, 28071 Madrid.

g) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

5. FICHERO: VOTO ACCESIBLE.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Voto accesible.

a.2) Finalidad y usos previstos: Según el Real Decreto 1612/2007, de 7 de diciembre, por el que se regula un procedimiento de voto accesible que facilita a las personas con discapacidad visual el ejercicio del derecho de sufragio, los electores con discapacidad visual que conozcan el sistema de lecto-escritura braille y tengan reconocido un grado de

minusvalía igual o superior al 33% o sean afiliados a la Organización Nacional de Ciegos Españoles, y deseen utilizar el procedimiento de voto accesible, pueden solicitar el kit de voto accesible, con material informativo rotulado en braille, para votar en las Elecciones a Cortes Generales, Parlamento Europeo, consultas directas al electorado y en las elecciones a asambleas legislativas a comunidades autónomas (en el caso de estas últimas de conformidad con lo previsto en la disposición adicional primera, apartado 2, de la Ley Orgánica 5/1985, de 19 de junio, de Régimen Electoral General, con las adaptaciones necesarias derivadas de su carácter y ámbito). El procedimiento de voto accesible requiere que dichos electores faciliten al Ministerio del Interior determinados datos personales. La Administración podrá requerir en cualquier momento la verificación de los datos personales del elector con discapacidad visual que haya comunicado su intención de utilizar el procedimiento de voto accesible.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Los electores con discapacidad visual que conozcan el sistema de lecto-escritura braille y tengan reconocido un grado de discapacidad igual o superior al 33% o sean afiliados a la Organización Nacional de Ciegos Españoles (ONCE), que deseen utilizar el procedimiento de voto accesible.

b.2) Procedencia y procedimiento de recogida: De conformidad con lo dispuesto en la Orden INT/3817/2007, de 21 de diciembre, por la que se desarrolla el Real Decreto 1612/2007, de 7 de diciembre, el elector interesado en utilizar el sistema de voto accesible deberá comunicar datos personales en el teléfono gratuito habilitado por el Ministerio del Interior para la recepción de solicitudes de voto accesible, entre el día de la convocatoria electoral y el vigésimo séptimo día posterior a la misma.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Datos de carácter identificativo: Nombre y apellidos, DNI, teléfono y dirección postal.

Datos especialmente protegidos relacionados con la salud de las personas: Grado de discapacidad visual igual o superior al 33%.

Características personales: Declaración de capacidad lectora en braille o afiliación a la ONCE.

c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios y transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: Instituto Nacional de Estadística (Oficina del Censo Electoral). Administración Electoral.

e) Órgano responsable del fichero: Dirección General de Política Interior.

f) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Política Interior y Procesos Electorales. C/ Amador de los Ríos, n.º 7, 28071 Madrid.

g) Nivel básico, medio o alto de seguridad que resulte exigible: Básico.

6. FICHERO: REGISTRO CENTRAL DE SANCIONES EN MATERIA DE VIOLENCIA, RACISMO, XENOFOBIA E INTOLERANCIA EN EL DEPORTE.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Registro Central de Sanciones en materia de violencia, racismo, xenofobia e intolerancia en el deporte.

a.2) Finalidad: Inscribir las sanciones impuestas en aplicación del Título II de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, y garantizar su cumplimiento.

a.3) Usos previstos: Registro de las sanciones firmes impuestas por las autoridades estatales o autonómicas competentes en materia de violencia, racismo, xenofobia e intolerancia en el deporte.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Entidades deportivas (definidas en el artículo 2.3 de la Ley 19/2007, de 11 de julio), personas organizadoras de competiciones y espectáculos deportivos o particulares que resulten sancionados por la comisión de las infracciones tipificadas en el Título II de la Ley 19/2007, de 11 de julio.

b.2) Procedencia y procedimiento de recogida: Las Autoridades estatales o autonómicas competentes en la materia comunicarán la resolución sancionadora y los datos objeto de inscripción cuando la sanción adquiera firmeza en vía administrativa.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Base de datos relacional.

Tipos de datos: Lugar y fecha del acontecimiento deportivo; clase de competición y contendientes; datos identificativos, de la entidad deportiva, organizador o particular sancionado; infracción cometida especificando el artículo de la Ley 19/2007, de 11 de julio, en el que está tipificada y, en su caso, las circunstancias modificativas de la responsabilidad; sanción o sanciones impuestas, especificando el artículo de la Ley 19/2007, de 11 de julio, en el que está tipificada, expresando con claridad su alcance temporal y geográfico, indicándose la fecha a partir de la que se inicie la ejecución efectiva de la sanción.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Consejo Superior de Deportes, Delegados y Subdelegados del Gobierno, órganos competentes de las comunidades autónomas, servicios de las Fuerzas y Cuerpos de Seguridad que la Dirección General de la Policía y de la Guardia Civil determine, así como las entidades deportivas y los particulares que tengan un interés directo y manifiesto.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Política Interior.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Política Interior.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

7. FICHERO: SEGUIMIENTO DE PROPUESTAS DE SANCIÓN Y EXPEDIENTES SANCIONADORES POR INFRACCIONES EN MATERIA DE VIOLENCIA, RACISMO, XENOFOBIA E INTOLERANCIA EN EL DEPORTE.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Seguimiento de propuestas de sanción y expedientes sancionadores por infracciones en materia de violencia, racismo, xenofobia e intolerancia en el deporte.

a.2) Finalidad: Seguimiento de las propuestas de sanción y de los expedientes sancionadores incoados por infracciones contenidas en el Título II de la Ley 19/2007, de 11 de julio.

a.3) Usos previstos: Usos administrativos y servir de base para la realización de estudios para la prevención de la violencia.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Entidades deportivas (definidas en el artículo 2.3 de la Ley 19/2007, de 11 de julio), propietarios de instalaciones deportivas, personas organizadoras de competiciones y espectáculos deportivos o particulares que hubieran participado en hechos tipificados como infracción y respecto de los cuales se hubiera propuesto una sanción tal y como se recoge en el artículo 74 del Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte, aprobado por el Real Decreto 203/2010, de 26 de febrero, o se hubiera abierto un expediente sancionador, conforme a lo dispuesto en el Título II de la Ley 19/2007, de 11 de julio.

b.2) Procedencia y procedimiento de recogida: Los datos de carácter personal se extraen de las actas de los coordinadores de seguridad en los espectáculos deportivos, reguladas por el artículo 74 del Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte, así como de las comunicaciones de las autoridades estatales o autonómicas competentes en la materia.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos:

Base de datos relacional.

Tipos de datos: Número de propuesta de sanción si la hubiera; lugar y fecha del acontecimiento deportivo; clase de competición y contendientes; datos identificativos de la entidad deportiva, organizador o particular propuesto para sanción; infracción cometida, especificando el artículo de la Ley 19/2007, de 11 de julio, en el que está tipificada; sanción o sanciones propuestas, especificando el artículo de la Ley 19/2007, de 11 de julio, en el que está tipificada, expresando con claridad su alcance temporal y geográfico; fecha de inicio y de resolución del expediente sancionador si lo hubiera, indicando la sanción o sanciones impuestas, así como su alcance temporal o geográfico; clase y fecha de interposición y de resolución de los recursos presentados si los hubiera; fecha de firmeza de la resolución sancionadora y de su inscripción en el Registro Central de sanciones deportivas en materia de violencia, racismo, xenofobia e intolerancia en el deporte.

c.2) Sistema de tratamiento: Automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: Autoridades estatales o autonómicas para el ejercicio de sus competencias en la materia, al amparo del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre.

e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.

f) Órgano responsable del fichero: Dirección General de Política Interior.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Dirección General de Política Interior.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Medio.

Secretaría General Técnica

1. FICHERO: JUGADORES PROHIBIDOS.

(Sin contenido)

2. FICHERO: EMPRESAS DE JUEGO.

(Sin contenido)

3. FICHERO: PROFESIONALES TAURINOS.
(Sin contenido)

4. FICHERO: EMPRESAS GANADERAS DE RESES DE LIDIA.
(Sin contenido)

5. FICHERO: ESCUELAS TAURINAS.
(Sin contenido)

6. FICHERO: RECURSOS, INDEMNIZACIONES, TRIBUNALES.

a) Identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos:

a.1) Identificación del fichero: Recursos, indemnizaciones, tribunales.
a.2) Finalidad: Seguimiento de los procedimientos originados por recursos administrativos, reclamaciones de responsabilidad patrimonial del Estado y relaciones con Tribunales.
a.3) Usos previstos: De orden interno, para la tramitación de los expedientes de las correspondientes materias y la gestión de las oportunas propuestas de Resolución. De orden externo, a efectos estadísticos.

b) Origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia:

b.1) Colectivo: Las personas recurrentes o reclamantes y las personas que intervengan en los procedimientos como terceros interesados.
b.2) Procedencia y procedimiento de recogida: Son suministrados por los Organismos recurridos y por los propios recurrentes o reclamantes y por terceros interesados que intervengan en los procedimientos, de conformidad con lo preceptuado en las normas procedimentales de aplicación.

c) Estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización:

c.1) Descripción de los datos: El fichero tienen tres capítulos distintos correspondientes a cada una de las materias: Recursos, Indemnizaciones y Relaciones con Tribunales. Los datos que se incluyen son la filiación (nombre y apellidos, DNI, domicilio), y las materias y circunstancias específicas de cada reclamación, o tipo de infracción y sanción que se recurre. El fichero incorpora datos especialmente protegidos: en materia de recursos, datos relativos a infracciones administrativas objeto de los recursos; en procedimientos de responsabilidad patrimonial, datos relativos a la salud de los reclamantes, que constituyen el fundamento de la pretensión indemnizatoria.
c.2) Sistema de tratamiento: Parcialmente automatizado.

d) Comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios: A los órganos judiciales que conozcan de los recursos contencioso-administrativos interpuestos contra resoluciones en materia de recursos y reclamaciones de responsabilidad patrimonial de la Administración, así como a la Abogacía General del Estado – Dirección del Servicio Jurídico del Estado, para la defensa de los mencionados recursos contencioso-administrativos.
e) Transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No se tiene previsto efectuar transferencias internacionales de datos.
f) Órgano responsable del fichero: Secretaría General Técnica.

g) Servicio o Unidad ante el que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Secretaría General Técnica. Subdirección General de Recursos. Amador de los Ríos, n.º 5, 28071 Madrid.

h) Nivel básico, medio o alto de seguridad que resulte exigible: Alto.

ANEXO III

Nombre del fichero: COMUNICACIONES DE VACACIONES.

Destino de los datos: Formateo de los soportes magnéticos a bajo nivel por desaparecer la finalidad para la que fue creado.

Secretaría de Estado de Seguridad

1. Nombre del fichero: Registro de correspondencia.

Destino de los datos: Integración de los datos en el nuevo fichero de Registro de correspondencia.

2. Nombre del fichero: Diligencias Policiales.

Destino de los datos: Formateo de los ficheros a bajo nivel por desaparecer la finalidad para la que fue creado.

3. Nombre del fichero: Sentencias judiciales.

Destino de los datos: Formateo de los soportes magnéticos a bajo nivel por desaparecer la finalidad para la que fue creado.

4. Nombre del fichero: Gibraltar.

Destino de los datos: Formateo de los soportes magnéticos a bajo nivel por desaparecer la finalidad para la que fue creado.

5. Nombre del fichero: Decomisos de divisas en aeropuertos.

Destino de los datos: Formateo de los soportes magnéticos a bajo nivel por desaparecer la finalidad para la que fue creado.

6. Nombre del fichero: Viajes.

Destino de los datos: Integración de los datos en el fichero Formación.

10 tris. Nombre Del fichero: Registro de correspondencia.

Destino de los datos: Integración de los datos en el nuevo fichero de Registro de correspondencia.

3. Nombre del fichero: SUQUICO.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

5. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Andalucía.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

6. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Aragón.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

7. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Baleares.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

8. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Canarias.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

9. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Cantabria.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

10. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Castilla y León.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

11. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Castilla-La Mancha.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

12. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Cataluña.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

13. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Ceuta.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

14. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en el País Vasco.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

15. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Asturias.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

16. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Extremadura.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

17. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Galicia.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

18. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en La Rioja.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

19. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Madrid.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

20. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Melilla.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

21. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Murcia.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

22. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en Navarra.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

23. Nombre del fichero: Registro Delegado de Sustancias Químicas Catalogadas en la Comunidad Valenciana.

Destino de los datos: Integración en el fichero Registro General de Operadores de Sustancias Químicas Catalogadas (RESUCA).

Dirección General de la Guardia Civil. Ámbito Guardia Civil.

23. Nombre del fichero: Gestión IRPF.

Destino de los datos: Integración de los datos en el nuevo fichero Retribuciones.

26. Nombre del fichero: Magallanes.

Destino de los datos: Integración de los datos en el nuevo fichero Ecofin.

27. Nombre del fichero: Medallas pensionadas.

Destino de los datos: Integración de los datos en el nuevo fichero Retribuciones.

28. Nombre del fichero: Nomiotros.

Destino de los datos: Integración de los datos en el nuevo fichero Retribuciones.

29. Nombre del fichero: Pagos a terceros.

Destino de los datos: Integración de los datos en el nuevo fichero Ecofin.

27. Nombre del fichero: Asuntos internos.

Destino de los datos: Destrucción.

32. Nombre del fichero: Haberes.

Destino de los datos: Integración de los datos en el nuevo fichero Retribuciones.

34. Nombre del fichero: Recursos nóminas.

Destino de los datos: Integración de los datos en el nuevo fichero Retribuciones.

36. Nombre del fichero: Retenciones judiciales.

Destino de los datos: Integración de los datos en el nuevo fichero Retribuciones.

41. Nombre del fichero: Sorolla.

Destino de los datos: Integración de los datos en el nuevo fichero Ecofin.

Secretaría General de Instituciones Penitenciarias

3. Nombre del fichero: Régimen especial.

Destino de los datos: Integración de los datos en el fichero FIES.

10. Nombre del fichero: Tratamiento.

Destino de los datos: Integración de los datos en el fichero SIP-Internos.

31. Nombre del fichero: Gestión de internos.

Destino de los datos: Integración de los datos en el fichero SIP-Internos.

Dirección General de Tráfico

88. Nombre del fichero: Concentrador de información de tráfico.

Destino de los datos: Destrucción.

INFORMACIÓN RELACIONADA

- Téngase en cuenta, con efectos de 13 de diciembre de 2016, que las alusiones hechas a la Subdirección General de Asociaciones, Documentación y Publicaciones se entenderán referidas a la Subdirección General de Asociaciones, Archivos y Documentación, según establece la disposición adicional 1 de la Orden INT/1865/2016, de 30 de noviembre. Ref. BOE-A-2016-11797.
- Véase, con efectos de 18 de mayo de 2012, en cuanto a las referencias hechas a los Centros Directivos del Ministerio del Interior, la disposición adicional 3 de la Orden INT/1031/2012, de 27 de abril. Ref. BOE-A-2012-6527.

§ 40

Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario. [Inclusión parcial]

Ministerio de Justicia e Interior
«BOE» núm. 40, de 15 de febrero de 1996
Última modificación: 26 de marzo de 2011
Referencia: BOE-A-1996-3307

[. . .]

REGLAMENTO PENITENCIARIO

TITULO I

Disposiciones generales

[. . .]

CAPITULO II

De los derechos y deberes de los internos

Artículo 4. *Derechos.*

1. La actividad penitenciaria se ejercerá respetando la personalidad de los internos y los derechos e intereses legítimos de los mismos no afectados por la condena, sin que pueda prevalecer discriminación alguna por razón de raza, sexo, religión, opinión, nacionalidad o cualquier otra condición o circunstancia personal o social.

2. En consecuencia, los internos tendrán los siguientes derechos:

a) Derecho a que la Administración penitenciaria vele por sus vidas, su integridad y su salud, sin que puedan, en ningún caso, ser sometidos a torturas, a malos tratos de palabra o de obra, ni ser objeto de un rigor innecesario en la aplicación de las normas.

b) Derecho a que se preserve su dignidad, así como su intimidad, sin perjuicio de las medidas exigidas por la ordenada vida en prisión. En este sentido, tienen derecho a ser designados por su propio nombre y a que su condición sea reservada frente a terceros.

c) Derecho al ejercicio de los derechos civiles, políticos, sociales, económicos y culturales, salvo cuando fuesen incompatibles con el objeto de su detención o el cumplimiento de la condena.

d) Derecho de los penados al tratamiento penitenciario y a las medidas que se les programen con el fin de asegurar el éxito del mismo.

e) Derecho a las relaciones con el exterior previstas en la legislación.

f) Derecho a un trabajo remunerado, dentro de las disponibilidades de la Administración penitenciaria.

g) Derecho a acceder y disfrutar de las prestaciones públicas que pudieran corresponderles.

h) Derecho a los beneficios penitenciarios previstos en la legislación.

i) Derecho a participar en las actividades del centro.

j) Derecho a formular peticiones y quejas ante las autoridades penitenciarias, judiciales, Defensor del Pueblo y Ministerio Fiscal, así como a dirigirse a las autoridades competentes y a utilizar los medios de defensa de sus derechos e intereses legítimos a que se refiere el capítulo V del Título II de este Reglamento.

k) Derecho a recibir información personal y actualizada de su situación procesal y penitenciaria.

[. . .]

CAPITULO III

Protección de los datos de carácter personal de los ficheros penitenciarios

Artículo 6. *Limitación del uso de la informática penitenciaria.*

1. Ninguna decisión de la Administración penitenciaria que implique la apreciación del comportamiento humano de los reclusos podrá fundamentarse, exclusivamente, en un tratamiento automatizado de datos o informaciones que ofrezcan una definición del perfil o de la personalidad del interno.

2. La recogida, tratamiento automatizado y cesión de los datos de carácter personal de los reclusos contenidos en los ficheros se efectuará de acuerdo con lo establecido en la legislación sobre protección de datos de carácter personal y sus normas de desarrollo.

3. Las autoridades penitenciarias responsables de los ficheros informáticos penitenciarios adoptarán las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal en ellos contenidos, así como para evitar su alteración, pérdida, tratamiento o acceso no autorizado, y estarán obligadas, junto con quienes intervengan en cualquier fase del tratamiento automatizado de este tipo de datos, a guardar secreto profesional sobre los mismos, incluso después de que haya finalizado su relación con la Administración penitenciaria.

4. La Administración penitenciaria podrá establecer ficheros de internos que tengan como finalidad garantizar la seguridad y el buen orden del establecimiento, así como la integridad de los internos. En ningún caso la inclusión en dicho fichero determinará por sí misma un régimen de vida distinto de aquél que reglamentariamente corresponda.

[. . .]

TITULO X

Del régimen disciplinario y de las recompensas

[. . .]

CAPITULO V

Prescripción y cancelación

[. . .]

Artículo 260. *Cancelación de anotaciones relativas a sanciones.*

1. Serán canceladas, de oficio o a instancia de parte, las anotaciones de las sanciones disciplinarias que obren en el expediente personal de los internos, cuando concurran los siguientes requisitos:

a) Transcurso de seis meses para las faltas muy graves, tres meses para las graves y un mes para las leves, a contar desde el cumplimiento de la sanción.

b) Que durante dichos plazos no haya incurrido el interno en nueva falta disciplinaria muy grave o grave.

2. También se cancelarán, de oficio o a instancia de parte, en el momento en que se produzca la excarcelación por la libertad provisional o definitiva del interno, las anotaciones de sanciones disciplinarias extinguidas automáticamente a que se refiere el artículo anterior.

3. Cuando fueren dos o más las faltas sancionadas en un mismo acto administrativo o sus plazos de cancelación corrieran simultáneamente, el cómputo se hará de forma conjunta, fijándose como fecha para su inicio la del cumplimiento de la sanción más reciente y tomándose como duración del plazo el que corresponda a la más grave de las infracciones a cancelar, transcurrido el cual se cancelarán todas las anotaciones pendientes en un solo acto.

4. En los casos de no cumplimiento de la sanción por razones médicas o de otro orden no imputables al interno, los plazos de cancelación comenzarán a contarse desde la fecha en que aquélla pudo haberse cumplido. Asimismo, en los casos del artículo 257, el plazo de cancelación comenzará a computarse desde la fecha en que la sanción quedó cumplida, por el abono de sanciones rectificadas en vía de recurso o reducidas o revocadas conforme a lo establecido en este Reglamento.

5. Dichos plazos no se interrumpirán por la interposición de recurso contra una nueva sanción disciplinaria, cancelándose las anteriores si transcurren sus plazos de cancelación antes de que la recurrida adquiera firmeza.

Artículo 261. *Reducción de los plazos de cancelación.*

Los plazos de cancelación podrán ser acortados hasta la mitad de su duración si, con posterioridad a la sanción y antes de completarse dichos plazos, el interno obtuviere alguna recompensa de las previstas en el artículo 263 de este Reglamento.

Artículo 262. *Efectos de la cancelación.*

La cancelación de la anotación de las sanciones lleva aparejada la de las faltas por las que se impusieron y situará al interno, desde el punto de vista disciplinario, en igual situación que si no hubiere cometido aquéllas.

[. . .]

§ 41

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Jefatura del Estado
«BOE» núm. 251, de 19 de octubre de 2007
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2007-18243

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de

Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter

general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un período de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. *Sujetos obligados.*

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos objeto de conservación.*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.
iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. *Obligación de conservar datos.*

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. *Período de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. *Normas generales sobre cesión de datos.*

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en el artículo 1.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. *Procedimiento de cesión de datos.*

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. *Protección y seguridad de los datos.*

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. *Excepciones a los derechos de acceso y cancelación.*

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. *Infracciones y sanciones.*

1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:

a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.

b) Son infracciones graves:

i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.

ii) La conservación de los datos por un período inferior al establecido en el artículo 5.

iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.

c) Son infracciones leves:

i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.

ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.

2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.

Disposición adicional única. *Servicios de telefonía mediante tarjetas de prepago.*

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la

seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Constituyen infracciones a lo previsto en la presente disposición, además de la previstas en el artículo 10, las siguientes:

a) Es infracción muy grave el incumplimiento de la llevanza del libro-registro referido.

b) Son infracciones graves la llevanza reiterada o sistemáticamente incompleta de dicho libro-registro así como el incumplimiento deliberado de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

c) Son infracciones leves la llevanza incompleta del libro-registro o el incumplimiento de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición cuando no se califiquen como infracciones muy graves o graves.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. *Vigencia del régimen de interceptación de telecomunicaciones.*

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.
h) Marcas temporales.
i) Información de localización.
j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.
b) Domicilio en el que el proveedor realiza las notificaciones.
Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:
c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).
d) Número de identificación del terminal.
e) Número de cuenta asignada por el proveedor de servicios Internet.
f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.
8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.
9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.
10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.
Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. *Competencia estatal.*

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Desarrollo reglamentario.*

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. *Formato de entrega de los datos.*

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. *Entrada en vigor.*

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 42

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 114, de 10 de mayo de 2014
Última modificación: 28 de abril de 2021
Referencia: BOE-A-2014-4950

[. . .]

TÍTULO III

Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas

[. . .]

CAPÍTULO III

Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas

[. . .]

Artículo 41. *Protección de los datos de carácter personal.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:

a) La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley.

b) La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.

c) La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas.

La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la Agencia Española de Protección de Datos que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Sin perjuicio de la obligación del proveedor de informar a los abonados o particulares afectados, si el proveedor no ha notificado ya al abonado o al particular la violación de los datos personales, la Agencia Española de Protección de Datos podrá exigirle que lo haga, una vez evaluados los posibles efectos adversos de la violación.

En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales.

Los operadores deberán llevar un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de las obligaciones de notificación reguladas en este apartado. Mediante real decreto podrá establecerse el formato y contenido del inventario.

A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La Agencia Española de Protección de Datos podrá adoptar directrices y, en caso necesario, dictar instrucciones sobre las circunstancias en que se requiere que el proveedor notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

[. . .]

CAPÍTULO IV

Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios

[. . .]

Artículo 48. *Derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados.*

1. Respecto a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial sin haber prestado su consentimiento previo e informado para ello.

b) A oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en la letra anterior y a ser informado de este derecho.

2. Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de tráfico, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio, para la devolución del cargo efectuado por el operador, para el pago de la factura o para que el operador pueda exigir su pago.

b) A que sus datos de tráfico sean utilizados para promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido, en la medida y durante el tiempo necesarios para tales servicios o promoción comercial únicamente cuando hubieran prestado su consentimiento informado para ello. Los usuarios finales dispondrán del derecho de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento y con efecto inmediato.

c) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado. Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico.

Los usuarios finales no podrán ejercer este derecho cuando se trate de llamadas de emergencia a través del número 112 o comunicaciones efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen por el Ministerio de Industria, Energía y Turismo.

3. Respecto a la protección de datos personales y la privacidad en relación con las guías de abonados, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A figurar en las guías de abonados.

b) A ser informados gratuitamente de la inclusión de sus datos en las guías, así como de la finalidad de las mismas, con carácter previo a dicha inclusión.

c) A no figurar en las guías o a solicitar la omisión de algunos de sus datos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor.

4. Lo establecido en las letras a) y c) del apartado 2 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 49. *Guías de abonados.*

1. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia.

A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

El Ministerio de Industria, Energía y Turismo deberá suministrar gratuitamente a las entidades que vayan a elaborar guías telefónicas de abonados, a las que presten el servicio de consulta telefónica sobre números de abonado y a las que presten los servicios de llamadas de emergencia, los datos que le faciliten los operadores, de conformidad con las condiciones que se establezcan mediante real decreto.

2. Se garantiza el acceso de los usuarios finales a los servicios de información sobre números de abonados, para cuya consecución el Ministerio de Industria, Energía y Turismo podrá imponer obligaciones y condiciones a las empresas que controlan el acceso a los usuarios finales en materia de prestación de servicios de información sobre números de abonado que deberán ser objetivas, equitativas, no discriminatorias y transparentes.

3. El Ministerio de Industria, Energía y Turismo adoptará, siempre que sea técnica y económicamente posible, medidas para garantizar el acceso directo de los usuarios finales al servicio de información sobre números de abonados de otro país comunitario mediante llamada vocal o SMS.

[. . .]

Disposición adicional cuarta. *Información confidencial.*

Las personas físicas o jurídicas que aporten a alguna Autoridad Nacional de Reglamentación datos o informaciones de cualquier tipo, con ocasión del desempeño de sus funciones y respetando la legislación vigente en materia de protección de datos y privacidad, podrán indicar, de forma justificada, qué parte de lo aportado consideran confidencial, cuya difusión podría perjudicarles, a los efectos de que sea declarada su confidencialidad. Cada Autoridad Nacional de Reglamentación decidirá, de forma motivada y a través de las resoluciones oportunas, sobre la información que, según la legislación vigente, resulte o no amparada por la confidencialidad.

[. . .]

§ 43

Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas

Ministerio de la Presidencia
«BOE» núm. 131, de 30 de mayo de 2009
Última modificación: sin modificaciones
Referencia: BOE-A-2009-8961

Desde la puesta en marcha del proceso de liberalización de las telecomunicaciones, tanto el derecho comunitario como el nacional han arbitrado mecanismos para que dicho proceso se produjera en un entorno de libre competencia y de pleno respeto a los derechos de los usuarios finales. En nuestro ordenamiento, la normativa básica a este respecto se contiene en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y en el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. En el ámbito comunitario, los derechos específicos de los usuarios de telecomunicaciones se recogen principalmente en la Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva del servicio universal). Este real real decreto, por lo tanto, es transposición de la citada directiva.

Por una parte, se establece el servicio universal de telecomunicaciones, que garantiza ciertas prestaciones a todos los ciudadanos, con independencia de su localización geográfica, a un precio asequible y con un nivel de calidad determinado. La garantía del servicio universal corresponde al operador designado para su prestación y su supervisión y control, al Ministerio de Industria, Turismo y Comercio.

Por otra parte, se reconocen a todos los usuarios finales de servicios de comunicaciones electrónicas, con independencia del operador con el que contraten, una serie de derechos, como el de disponer de un contrato en el que figuren las condiciones que se le aplican, el derecho a darse de baja en cualquier momento, el de ser indemnizado en caso de interrupción del servicio, o el de recibir facturación detallada, entre muchos otros.

Esta protección específica del usuario de telecomunicaciones se añade, además, a la que todo consumidor y usuario tiene conforme a la legislación general de protección de los consumidores, en particular el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, así como la normativa autonómica dictada en la materia. La complementariedad de ambos regímenes, convierte a las telecomunicaciones en uno de los sectores cuyos usuarios gozan de un mayor nivel de protección.

El Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, no sólo reconoce un importante número de derechos a los usuarios finales, sino que, además, establece un

eficaz mecanismo para su protección: el procedimiento de resolución de controversias entre usuarios finales y operadores, de manera que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información dispone de competencia para la resolución vinculante de conflictos entre ambas partes.

Tras más de tres años de experiencia en la aplicación del régimen de derechos los usuarios finales de telecomunicaciones, para avanzar en su protección, el Acuerdo de Consejo de Ministros de 14 de agosto de 2008, sobre medidas de reforma estructural y de impulso de la financiación de las pequeñas y medianas empresas contiene, entre otras medidas, un mandato para la aprobación de esta norma.

Sin perjuicio de las competencias de las Comunidad Autónomas sobre protección general de consumidores y usuarios, este real decreto regula el régimen de protección específica de estos usuarios de servicios de comunicaciones electrónicas. Manteniendo los derechos existentes, incluye nuevas garantías que regirán, a partir de su entrada en vigor, sus relaciones con los operadores, elevando así el alto nivel de protección de que eran titulares hasta el momento.

Se recogen las prestaciones que, como servicio universal, deben garantizarse por el operador designado a todos los ciudadanos, incluyendo las medidas específicas para el acceso al servicio telefónico fijo por personas con discapacidad.

En los aspectos contractuales, se han introducido mecanismos que garanticen la necesaria coordinación entre los procedimientos regulados para el acceso a las redes por los operadores y las relaciones contractuales entre éstos y los usuarios finales. Con ello, se dotan de mayores garantías jurídicas para los usuarios los procesos de altas, bajas y de cambio de operador. Se recogen hasta quince extremos que deberán figurar en los contratos, en garantía de la información a los usuarios finales de las condiciones que se le aplican.

Se refuerza la protección de los usuarios finales en los procesos de alta, tanto en la información que reciben como en las prestaciones recibidas. A este respecto, estará prohibido publicitar velocidades de acceso a Internet superiores a las que admita la tecnología utilizada. Asimismo, los operadores deberán informar a los usuarios sobre los factores que pueden limitar la velocidad efectiva que experimentan.

Asimismo, se fija en dos días, previéndose su reducción a 24 horas, el plazo en que la portabilidad debe llevarse a efecto, en línea con las propuestas sobre reducción de plazos para la portabilidad que se están llevando a cabo en el seno de la Unión Europea, dentro de los trabajos para la elaboración del nuevo marco comunitario regulador de las comunicaciones electrónicas. Esta medida permitirá una mayor agilidad en los procesos de cambio de operador, y, con ello, favorecer la competencia. Asimismo, se prevé continuar con la mejora de los procedimientos de portabilidad, sin que ello suponga un incremento en el coste para el usuario final.

Se regulan las obligaciones de transparencia de los operadores, tanto en relación con las condiciones contractuales que aplican a los usuarios finales como con los niveles de calidad conseguidos. De este modo, se refuerza la capacidad de elección de los usuarios, que podrá comparar entre niveles de calidad conseguidos por los distintos operadores.

El usuario final tendrá derecho a ser indemnizado por las interrupciones del servicio que sufra. Este real decreto contiene reglas específicas para la determinación de la cuantía de la compensación, distinguiendo el servicio de acceso a Internet del de telefonía. La práctica de la compensación deberá ser automática si su cuantía es superior a un euro para el servicio telefónico o si supera las seis horas en horario de 8.00 a 22.00 para el de acceso a Internet.

Los usuarios finales de todos los servicios de comunicaciones electrónicas tendrán derecho a recibir facturas por los cargos en que incurran. A este respecto, este real decreto contiene el desglose que deberá contener la factura del servicio telefónico, tanto fijo como móvil. En el supuesto de que en la factura de un servicio de comunicaciones electrónicas se contengan importes correspondientes a bienes o servicio que no tengan tal naturaleza, se establece que el impago de estos últimos no podrá acarrear la suspensión del servicio de comunicaciones electrónicas. Este derecho del usuario final constituye una eficaz protección, de modo que la continuidad del servicio no podrá verse amenazada por posibles impagos de bienes o servicios distintos.

Los derechos de los usuarios finales se corresponden con las correlativas obligaciones que deben exigírseles en la contratación y uso de los servicios de comunicaciones electrónicas. En este sentido, deberán utilizar los servicios para los fines previstos en el contrato, evitando un uso fraudulento, cumplir con la contraprestación prevista por el suministro de los servicios o utilizar terminales que hayan evaluado su conformidad según la normativa vigente.

Finalmente, este amplio catálogo de derechos se completa con importantes mecanismos de protección del usuario, tanto en orden a su acreditación como a su reparación en caso de incumplimiento.

Por una parte, se regulan los requisitos que deben reunir los servicios de atención al cliente de los operadores. Esta regulación se encamina a garantizar una atención eficaz hacia los usuarios finales. Se refuerza el derecho de estos a disponer de una acreditación documental de todas las gestiones de relevancia contractual que realicen telefónicamente.

Por otra parte, se recoge en este real decreto la regulación del procedimiento de resolución de controversias entre usuarios finales y operadores. Estos podrán dirigir reclamaciones a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información que, en el plazo máximo de seis meses, las resolverá de manera vinculante para el operador, ordenando las medidas que resulten necesarias para restituir a los usuarios sus derechos vulnerados. Con ello se está dando cumplimiento al artículo 34 de la Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva del servicio universal). Este procedimiento de resolución de controversias se entiende sin perjuicio de las medidas sancionadoras que procedan en caso de incumplimiento de la normativa de protección de los usuarios finales.

En su virtud, a propuesta del Ministro de Industria, Turismo y Comercio y de la Ministra de Sanidad y Política Social, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 22 de mayo de 2009,

DISPONGO:

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. *Objeto y definiciones.*

1. Este real decreto tiene por objeto la aprobación de la Carta de derechos del usuario de los servicios de comunicaciones electrónicas, en desarrollo del artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. A los efectos de este real decreto se entiende por:

a) «Abonado»: cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público, para la prestación de dichos servicios.

b) «Bucle local»: el circuito físico que conecta el punto de terminación de la red en las dependencias del abonado a la red de distribución principal o instalación equivalente de la red pública de telefonía fija.

c) «Operador»: la persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad

d) «Servicio de comunicaciones electrónicas»: el prestado por lo general a cambio de una remuneración, que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad

de la información definidos en el artículo 1 de la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas.

e) «Servicio de tarificación adicional»: los que hayan sido declarados como tales por resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, en razón de la existencia de una facturación superior al coste del servicio de comunicaciones electrónicas y en interés de una especial protección de los derechos de los usuarios.

f) «Usuario final» el usuario que no explota redes públicas de comunicaciones ni presta servicios de comunicaciones electrónicas disponibles al público, ni tampoco los revende.

Artículo 2. *Ámbito de aplicación.*

Serán titulares de los derechos reconocidos en este real decreto, en las condiciones establecidas en el mismo, los usuarios finales de servicios de comunicaciones electrónicas. Los operadores estarán obligados a respetar los derechos reconocidos en esta disposición.

Los derechos reconocidos en este real decreto son adicionales y compatibles con lo dispuesto en otras normas aplicables y, en especial, en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, y, asimismo, en la legislación dictada por las Comunidades Autónomas en el ejercicio de sus competencias sobre protección general de consumidores y usuarios.

TÍTULO II

CARTA DE DERECHOS DEL USUARIO DE LOS SERVICIOS DE COMUNICACIONES ELECTRÓNICAS

Artículo 3. *Derechos de los usuarios finales.*

Los usuarios finales de servicios de comunicaciones electrónicas serán titulares, además de los derechos establecidos en el artículo 8 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, de los siguientes derechos, en las condiciones establecidas en este real decreto:

a) Derecho a obtener una conexión a la red telefónica públicas desde una ubicación fija, que posibilite el acceso funcional a Internet, y acceder a la prestación del servicio telefónico, así como al resto de prestaciones incluidas en el servicio universal, con independencia de su localización geográfica, a un precio asequible y con una calidad determinada.

b) Derecho a celebrar contratos y a rescindirlos, así como a cambiar de operador de forma segura y rápida, con conservación del número telefónico. En particular, incluye el derecho a resolver el contrato anticipadamente, sin penalización, en supuestos de modificación del mismo por el operador por motivos válidos especificados en aquél y sin perjuicio de otras causas de resolución unilateral.

c) Derecho a la información veraz, eficaz, suficiente, transparente y actualizada sobre las condiciones ofrecidas por los operadores y las garantías legales.

d) Derecho recibir servicios de comunicaciones electrónicas con garantías de calidad, así como a recibir información comparable, pertinente y actualizada sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público.

e) Derecho a la continuidad del servicio, y a una indemnización en caso de interrupciones.

f) Derecho a una facturación desglosada, a la desconexión de determinados servicios y a elegir el medio de pago de los servicios entre los comúnmente utilizados en el tráfico comercial.

g) Derecho a una atención eficaz por el operador.

h) Derecho a unas vías rápidas y eficaces para reclamar.

i) Derecho a prestaciones especiales para personas con discapacidad y de renta baja.

j) Derecho a una especial protección en la utilización de servicios de tarificación adicional.

k) Derecho a la protección de los datos de carácter personal.

CAPÍTULO I

Derecho al acceso a la red telefónica fija, con una conexión que garantice el acceso funcional a Internet, así como al resto de prestaciones incluidas en el servicio universal, a un precio asequible y con una calidad determinada

Artículo 4. *Servicios que se incluyen en el ámbito del servicio universal.*

1. Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible.

2. Bajo el concepto de servicio universal se garantiza, en los términos y condiciones que se establecen en el título III del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, lo siguiente:

a) Que todos los usuarios finales puedan obtener una conexión a la red telefónica pública desde una ubicación fija y acceder a la prestación del servicio telefónico disponible al público, siempre que sus solicitudes se consideren razonables. La conexión deberá ofrecer la posibilidad de establecer comunicaciones de datos a velocidad suficiente para acceder de forma funcional a Internet.

b) Que se ponga a disposición de los abonados al servicio telefónico disponible al público una guía general de números de abonados. Asimismo, que se ponga a disposición de todos los usuarios finales de dicho servicio un servicio de información general o consulta telefónica sobre números de abonados.

c) Que exista una oferta suficiente de teléfonos públicos de pago en todo el territorio nacional.

d) Que los usuarios finales con discapacidad tengan acceso al servicio telefónico disponible al público desde una ubicación fija en condiciones equiparables a las que se ofrecen al resto de usuarios finales.

e) Que las personas con necesidades sociales especiales, dispongan de opciones o paquetes de tarifas que difieran de las aplicadas en condiciones normales de explotación comercial y que les permitan tener acceso al servicio telefónico disponible al público desde una ubicación fija y hacer uso de éste.

f) Que se apliquen, cuando proceda, opciones tarifarias especiales o limitaciones de precios, tarifas comunes, equiparación por zonas u otros regímenes similares, de acuerdo con condiciones transparentes, públicas y no discriminatorias.

CAPÍTULO II

Derecho a celebrar contratos y a rescindirlos, así como a cambiar de operador

Artículo 5. *Celebración de los contratos.*

1. Los usuarios finales de servicios de comunicaciones electrónicas tendrán derecho a celebrar contratos con los operadores, con el contenido mínimo previsto en el artículo 8, y a recibir el servicio en las condiciones pactadas con ellos.

La formalización y entrega del contrato se regirá por lo dispuesto en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, sin perjuicio de otras formalidades adicionales que, en su caso, se establezcan en la regulación de la portabilidad y la preselección.

2. Los operadores no podrán acceder a la línea de un usuario final sin su consentimiento expreso e inequívoco.

3. En relación con el servicio de banda ancha para acceder a Internet, el operador no podrá aplicar al usuario final una oferta cuya velocidad máxima publicitada sea superior a la velocidad máxima que admita la tecnología utilizada sobre su bucle local o en el enlace de acceso.

El operador deberá informar al usuario final, antes de su contratación, de los factores relevantes que limitan la velocidad efectiva que puede experimentar el usuario, diferenciando aquellos sobre los que tiene control el operador de los ajenos al mismo.

A los efectos de lo establecido en el párrafo anterior, mediante resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información se podrá establecer el contenido mínimo y demás condiciones que los operadores deben cumplir al informar a los usuarios, con carácter previo a la contratación.

Artículo 6. *Depósitos de garantía.*

1. Los operadores que presten el servicio telefónico disponible al público desde una ubicación fija únicamente podrán exigir a los abonados a dicho servicio la constitución de un depósito de garantía, tanto en el momento de contratar como durante la vigencia del contrato, en los siguientes supuestos:

a) En los contratos de abono al servicio telefónico disponible al público desde una ubicación fija solicitado por personas físicas o jurídicas que sean o hayan sido con anterioridad abonados al servicio y hubieran dejado impagados uno o varios recibos, en tanto subsista la morosidad.

b) En los contratos de abono al servicio telefónico disponible al público desde una ubicación fija cuyos titulares tuvieran contraídas deudas por otro u otros contratos de abono, vigentes o no en ese momento, o bien que de modo reiterado se retrasen en el pago de los recibos correspondientes.

c) Para los abonados al servicio telefónico disponible al público desde una ubicación fija titulares de líneas que dan servicio a equipos terminales de uso público para su explotación por terceros en establecimientos públicos.

d) En los contratos para la prestación de servicios de tarificación adicional formalizados entre los operadores de red y los prestadores de dichos servicios.

e) En aquellos supuestos en que excepcionalmente lo autorice la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a petición de los operadores, en casos de existencia de fraude o tipos de fraude detectados de modo cierto y para asegurar el cumplimiento del contrato por los usuarios finales.

2. La cuantía de los depósitos, su duración, el procedimiento para su constitución y devolución, así como si serán o no remunerados se determinará mediante orden del Ministro de Industria, Turismo y Comercio.

3. A los depósitos de garantía para servicios distintos al telefónico desde una ubicación fija se aplicará lo dispuesto en los correspondientes contratos de abono o de prepago con sujeción, en todo caso, a lo previsto en la normativa general sobre protección de los consumidores y usuarios.

Artículo 7. *Extinción de los contratos.*

El contrato se extinguirá por las causas generales de extinción de los contratos y, especialmente, por voluntad del abonado, comunicándolo previamente al operador con una antelación mínima de dos días hábiles al momento en que ha de surtir efectos.

El operador se abstendrá de facturar y cobrar cualquier cantidad que se haya podido devengar, por causa no imputable al usuario final, con posterioridad al plazo de dos días en que debió surtir efectos la baja.

El procedimiento habilitado por el operador para que el consumidor haga uso de este derecho se ajustará a lo previsto en el artículo 26.2 de este real decreto, garantizando en todo caso al usuario la constancia del contenido de su solicitud de baja en el servicio.

Artículo 8. *Contenido de los contratos.*

1. Los contratos que celebren los usuarios finales de servicios de comunicaciones electrónicas con los operadores precisarán, como mínimo, los siguientes aspectos:

a) El nombre o razón social del operador y el domicilio de su sede o establecimiento principal.

b) El teléfono de atención al cliente y, en su caso, otras vías de acceso a dicho servicio.

c) Las características del servicio de comunicaciones electrónicas ofrecido, la descripción de cada una de las prestaciones incluidas en el contrato, con la indicación de qué conceptos se incluyen respectivamente en la cuota de abono y, en su caso, en otras cuotas. Asimismo, figurará el derecho de desconexión, en su caso, y su modo de ejercicio, en los supuestos del artículo 24.

d) Los niveles individuales de calidad de servicio establecidos conforme a los parámetros y métodos de medida que, en su caso, determine el Ministerio de Industria, Turismo y Comercio, así como las indemnizaciones asociadas al incumplimiento de los compromisos de calidad y si éstas se ofrecen de forma automática por el operador o previa petición del usuario final. Entre dichos parámetros figurará el relativo al tiempo de suministro de la conexión inicial

e) Precios y otras condiciones económicas de los servicios. Se incluirán en el contrato los precios generales relativos al uso del servicio, desglosando, en su caso, los distintos conceptos que los integren y los servicios incluidos en los mismos. Asimismo, se especificarán las modalidades de obtención de información actualizada sobre todas las tarifas aplicables y las cuotas de mantenimiento.

f) Período contractual, indicando, en su caso, la existencia de plazos mínimos de contratación y de renovación, así como, en su caso, las consecuencias de su posible incumplimiento.

g) El detalle, en su caso, de los vínculos existentes entre el contrato de servicio de comunicaciones electrónicas y otros contratos, como los relativos a la adquisición de aparatos terminales.

h) Política de compensaciones y reembolsos, con indicación de los mecanismos de indemnización o reembolso ofrecidos, así como el método de determinación de su importe.

i) Características del servicio de mantenimiento incluido y otras opciones

j) Procedimientos de resolución de litigios de entre los previstos en el artículo 27, con inclusión, en su caso, de otros que haya creado el propio operador.

k) Causas y formas de extinción y renovación del contrato de abono, entre las que deberá figurar expresamente, además de las causas generales de extinción de los contratos, la de la voluntad unilateral del abonado, comunicada al operador con una antelación mínima de dos días al que ha de surtir efectos, así como el procedimiento para ejercitar este derecho.

l) Dirección postal y de correo electrónico del departamento o servicio especializado de atención al cliente a que se refiere el artículo 26, teléfonos propios del operador y, en su caso, página web, o cualquier otro medio adicional habilitado por el operador, a efectos de la presentación de quejas, reclamaciones, gestiones con incidencia contractual y peticiones por parte del abonado, especificando un procedimiento sencillo, gratuito y sin cargos adicionales, que permita la presentación de las mismas y su acreditación.

m) Página de Internet en que figura la información que el operador debe publicar, conforme al artículo 12.

n) Reconocimiento del derecho a la elección del medio de pago, de entre los comúnmente utilizados en el tráfico comercial.

o) Información referida al tratamiento de los datos de carácter personal del cliente, en los términos exigidos por la legislación vigente en esta materia.

p) Información al cliente en materia de protección de los datos personales en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas, en los supuestos y con el contenido exigido por las disposiciones del capítulo I del título V del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, cuando proceda.

2. El contenido mínimo previsto en el apartado anterior deberá, constar, igualmente, en las condiciones generales y particulares de los contratos de los usuarios finales de servicios

de comunicaciones electrónicas, en la modalidad de prepago. En dichas condiciones generales figurará el procedimiento, para conocer el saldo y el detalle del consumo, así como para la recarga.

Artículo 9. *Modificaciones contractuales.*

1. Los contratos de servicios de comunicaciones electrónicas sólo podrán ser modificados por los motivos válidos expresamente previstos en el contrato.

2. El usuario final tendrá derecho a resolver anticipadamente y sin penalización alguna el contrato en los supuestos previstos en el apartado anterior.

3. Los operadores deberán notificar al usuario final las modificaciones contractuales con una antelación mínima de un mes, informando expresamente en la notificación de su derecho a resolver anticipadamente el contrato sin penalización alguna.

Artículo 10. *Procesos de cambio de operador.*

1. Con independencia de los mecanismos que utilicen los operadores para el acceso a las redes, los procesos de cambio de operador se realizarán, con carácter general, a través de la baja del usuario final con el operador de origen y el alta con el de destino. A los efectos de tramitación de la baja, el abonado deberá comunicarla directamente al operador de origen conforme al procedimiento que figure en el contrato.

No obstante lo establecido en el párrafo anterior, la recepción por el operador de origen de una solicitud válida de cambio de operador con conservación de número implicará la baja con dicho operador de todos los servicios asociados al servicio telefónico identificado por la numeración portada. La baja surtirá efectos a partir del momento en que el operador de origen deje de prestar efectivamente el servicio.

Asimismo, en caso de que un operador preste servicios soportados por una línea de acceso de titularidad de otro operador, una notificación por éste a aquél, a través de los procedimientos regulados para el acceso a las redes, de baja técnica que haga imposible la continuación en la prestación del servicio deberá ser considerada por ese operador como una baja contractual, una vez haya dejado de tener acceso a la red.

2. Los abonados al servicio telefónico disponible al público tendrán derecho a conservar, previa solicitud, los números que les hayan sido asignados en los términos establecidos en el Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración.

Artículo 11. *Aprobación y notificación de contratos y otras condiciones.*

1. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información aprobará, previo informe de la Comisión del Mercado de las Telecomunicaciones, de la Agencia Española de Protección de Datos y del Instituto Nacional del Consumo, y con audiencia de las asociaciones de consumidores y usuarios, a través del Consejo de Consumidores y Usuarios, con carácter previo a su utilización, las condiciones generales de contratación relativas a la prestación de servicios de comunicaciones electrónicas que estén sujetos a obligaciones de servicio público. En caso de que en la tramitación del procedimiento de aprobación, ésta vaya a denegarse o se vayan a imponer condiciones, deberá otorgarse un trámite de audiencia al operador.

Los contratos respetarán los niveles mínimos de calidad que, en su caso, se establezcan.

2. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información aprobará con carácter previo a su utilización, y con informe de la Comisión de supervisión de los servicios de tarificación adicional, de la Agencia Española de Protección de Datos, del Consejo de Consumidores y Usuarios y de la Comisión del Mercado de las Telecomunicaciones, las condiciones generales de contratación relativas a la prestación de servicios de tarificación adicional, definidos en el artículo 30 y establecerá, en su caso, las condiciones imperativas aplicables.

En caso de que en la tramitación del procedimiento de aprobación, ésta vaya a denegarse o se vayan a imponer condiciones, deberá otorgarse un trámite de audiencia al operador.

3. Las condiciones generales de contratación distintas a las mencionadas en los apartados anteriores y sus actualizaciones y modificaciones deberán ser comunicados, con al menos un mes de antelación a su entrada en vigor, al Ministerio de Industria, Turismo y Comercio, a la Comisión del Mercado de las Telecomunicaciones, al Instituto Nacional del Consumo, a la Agencia Española de Protección de Datos y al Consejo de Consumidores y Usuarios. Este último organismo las pondrá a disposición de las asociaciones de consumidores y usuarios integradas en él.

Los operadores que presten las facilidades de identificación de la línea llamante y de la línea conectada deberán comunicar la información relativa a la prestación de dichas facilidades a las entidades citadas en el párrafo anterior.

Asimismo, los operadores deberán comunicar a dichas entidades, con diez días naturales de antelación a su entrada en vigor, las tarifas que no deban figurar obligatoriamente en los contratos con los abonados.

CAPÍTULO III

Derecho a la información veraz, eficaz, suficiente, transparente y actualizada sobre las concisiones ofrecidas por los operadores y las garantías legales

Artículo 12. *Derecho a información veraz, eficaz, suficiente, transparente y actualizada.*

1. Antes de contratar, los operadores de comunicaciones electrónicas deben poner a disposición del usuario final de forma clara, comprensible y adaptada a las circunstancias la información veraz, eficaz, suficiente y transparente sobre las características del contrato, en particular sobre sus condiciones jurídicas y económicas y de los servicios objeto del mismo.

Los operadores de servicios de comunicaciones electrónicas publicarán sus condiciones generales de contratación en un lugar fácilmente accesible de su página de Internet. Asimismo, facilitarán dichas condiciones por escrito, si así lo solicita un usuario final, que no deberá afrontar gasto alguno por su recepción, e informarán sobre ellas en el teléfono de atención al público, que tendrá el coste máximo del precio ordinario del servicio de telecomunicaciones sin recargo.

2. Los operadores que presten el servicio telefónico disponible al público facilitarán, por los medios establecidos en el apartado anterior, la siguiente información:

a) Su nombre o razón social y el domicilio de su sede o establecimiento principal.

b) En relación con el servicio telefónico disponible al público que prestan:

1.º Descripción de los servicios ofrecidos, indicando todos los conceptos que se incluyen en la cuota de alta, en la cuota de abono y en otras cuotas de facturación periódica.

2.º Tarifas generales, que incluyan la cuota de acceso y todo tipo de cuota de utilización y mantenimiento, con inclusión de información detallada sobre reducciones y tarifas especiales y moduladas.

3.º Política de compensaciones y reembolsos, con detalles concretos de los mecanismos de indemnización y reembolso ofrecidos.

4.º Tipos de servicios de mantenimiento incluidos y otras opciones.

5.º Condiciones normales de contratación, incluido el plazo mínimo, en su caso.

c) Procedimientos de resolución de conflictos, con inclusión de los creados por el propio operador.

d) Información, en su caso, acerca de los derechos en relación con el servicio universal, incluidas las facilidades y servicios citados en el artículo 35 del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril

3. Los operadores que presten las facilidades de identificación de la línea llamante y de la línea conectada deberán comunicar la información relativa a la prestación de dichas facilidades por los medios indicados en el apartado 1 de este artículo.

4. Mediante orden del Ministro de Industria, Turismo y Comercio podrán establecerse los términos conforme a los cuales deberá publicarse la información a que se refiere este artículo, con objeto de posibilitar la comparación.

Artículo 13. *Comunicaciones comerciales.*

Las comunicaciones comerciales en las que se haga referencia a ofertas sujetas a limitaciones temporales o de otra índole deben informar, de una forma adecuada a las limitaciones del medio utilizado para la comunicación, de tales limitaciones. Las limitaciones temporales a las que, en su caso, estén sujetas las ofertas deberán ser razonables.

CAPÍTULO IV

Derecho a recibir servicios de telecomunicaciones con garantías de calidad, así como a recibir información comparable, pertinente y actualizada sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público

Artículo 14. *Obligaciones sobre calidad y facturación.*

1. Los operadores que presten servicios de comunicaciones electrónicas publicarán información detallada, comparable, pertinente, fácilmente comprensible, accesible y actualizada sobre la calidad de los servicios que presten. Esta información tendrá que constar en la página de Internet del operador. Los parámetros y métodos para su medición deberán estar disponibles para los consumidores que sean personas físicas y otros usuarios finales.

A tales efectos, el Ministro de Industria, Turismo y Comercio podrá especificar, mediante orden, entre otros elementos, los parámetros de calidad de servicio que habrán de cuantificarse, así como el contenido y formato de la información que deberá hacerse pública, las modalidades de su publicación y las condiciones orientadas a garantizar la fiabilidad y la posibilidad de comparación de los datos, incluida la realización anual de auditorías.

2. Los prestadores de servicios de comunicaciones electrónicas disponibles al público deberán facilitar al Ministerio de Industria, Turismo y Comercio, previa petición, la información de calidad de servicio que le requiera para la publicación de síntesis comparativas y para el control y seguimiento de las condiciones de prestación de los servicios y de las obligaciones de carácter público. Dicha información se deberá referir a los parámetros establecidos por la orden ministerial a la que se refiere el apartado anterior. Adicionalmente, se podrá establecer la obligación de informar sin necesidad de petición previa cuando se produzcan degradaciones importantes de la calidad de servicio, en los términos que allí se establezcan.

3. Mediante orden del Ministro de Industria, Turismo y Comercio podrán establecerse, asimismo, mecanismos para garantizar la exactitud de la facturación realizada, que podrán incluir, en particular, la necesidad de que determinadas categorías de operadores, como aquellos que prestan servicio con tarificación en función de la duración de la conexión, del volumen de información o de la distancia, tengan que acreditar que sus sistemas de medida, de tarificación y de gestión de la facturación cumplan con normas de aseguramiento de la calidad como las de la familia ISO 9000.

CAPÍTULO V

Derecho a la continuidad del servicio y a ser indemnizado en caso de Interrupción

Artículo 15. *Derecho a indemnización por la interrupción temporal del servicio telefónico disponible al público.*

1. Cuando, durante un período de facturación, un abonado sufra interrupciones temporales del servicio telefónico disponible al público, el operador deberá indemnizar con una cantidad que será, al menos, igual a la mayor de las dos siguientes:

a) El promedio del importe facturado por todos los servicios interrumpidos durante los tres meses anteriores a la interrupción, prorrateado por el tiempo que haya durado la interrupción. En caso de una antigüedad inferior a tres meses, se considerará el importe de la factura media en las mensualidades completas efectuadas o la que se hubiese obtenido

en una mensualidad estimada de forma proporcional al período de consumo efectivo realizado.

b) Cinco veces la cuota mensual de abono o equivalente vigente en el momento de la interrupción, prorrateado por el tiempo de duración de ésta.

El operador estará obligado a indemnizar automáticamente al abonado, en la factura correspondiente al período inmediato al considerado cuando la interrupción del servicio suponga el derecho a una indemnización por importe superior a 1 euro. En la factura correspondiente se hará constar la fecha, duración y cálculo de la cuantía de la indemnización que corresponde al abonado.

En el caso de abonados sujetos a modalidades prepago, el correspondiente ajuste en el saldo se realizará en un plazo no superior al del resto de abonados.

En interrupciones por causas de fuerza mayor, el operador se limitará a compensar automáticamente al abonado con la devolución del importe de la cuota de abono y otras independientes del tráfico, prorrateado por el tiempo que hubiera durado la interrupción.

El contrato de abono del servicio telefónico deberá recoger los términos y condiciones en que se dará cumplimiento a esta obligación.

2. No será de aplicación lo dispuesto en el apartado anterior cuando la interrupción temporal esté motivada por alguna de las causas siguientes:

a) Incumplimiento grave por los abonados de las condiciones contractuales, en especial en caso de fraude o mora en el pago que dará lugar a la aplicación de la suspensión temporal e interrupción de los artículos 19 y 20, respectivamente. En todo caso, la suspensión temporal o interrupción afectará únicamente al servicio en el que se hubiera producido el fraude o mora en el pago.

b) Por los daños producidos en la red debido a la conexión por el abonado de equipos terminales que no hayan evaluado la conformidad, de acuerdo con la normativa vigente.

c) Incumplimiento del código de conducta por parte de un usuario que preste servicios de tarificación adicional, cuando la titularidad del contrato de abono corresponda a este último.

3. La indemnización prevista en este artículo se entiende sin perjuicio de la responsabilidad por daños que se produzcan a los usuarios finales, que se exigirá conforme a lo previsto en el artículo 18.

Artículo 16. *Derecho a compensación por la interrupción temporal del servicio de acceso a Internet.*

1. Cuando, durante un período de facturación, un abonado sufra interrupciones temporales del servicio de acceso a Internet, el operador deberá compensar al abonado con la devolución del importe de la cuota de abono y otras cuotas fijas, prorrateadas por el tiempo que hubiera durado la interrupción. A estos efectos, el operador estará obligado a indemnizar automáticamente al abonado, en la factura correspondiente al período inmediato al considerado, cuando la interrupción del servicio, se haya producido de manera continua o discontinua, y sea superior a seis horas en horario de 8 a 22. En la factura correspondiente se hará constar la fecha, duración y cálculo de la cuantía de la compensación que corresponde al abonado.

El contrato de abono del servicio de acceso a Internet deberá recoger los términos y condiciones en que se dará cumplimiento a esta obligación.

2. No será de aplicación lo dispuesto en el apartado anterior cuando la interrupción temporal esté motivada por alguna de las causas siguientes:

a) Incumplimiento grave por los abonados de las condiciones contractuales.

b) Daños producidos en la red debido a la conexión por el abonado de equipos terminales que no hayan evaluado la conformidad, de acuerdo con la normativa vigente.

3. A los efectos del derecho a indemnización o compensación por la interrupción del servicio de acceso a Internet, y para la determinación de su cuantía, cuando un operador incluya en su oferta la posibilidad de contratar conjuntamente servicios de telefonía y otros servicios como el de acceso a Internet, podrá indicar en su oferta la parte del precio que corresponde a cada servicio. De no hacerlo, se considerará que el precio de cada uno es el proporcional al de su contratación por separado. Si el operador no comercializara los

servicios por separado, se considerará que el precio correspondiente al servicio de acceso a Internet es del 50 por ciento del precio total.

4. La compensación prevista en este artículo se entiende sin perjuicio de la responsabilidad por daños que se produzcan a los usuarios finales, que se exigirá conforme a lo previsto en el artículo 18.

Artículo 17. *Determinación de los usuarios afectados por una interrupción del servicio telefónico móvil o de acceso a Internet móvil.*

Se entenderá que una interrupción del servicio en una zona afecta a un abonado cuando se dé alguna de las siguientes circunstancias:

a) El operador conoce a través de sus sistemas de información que dicho abonado se encontraba en la zona afectada en el momento de la interrupción.

b) La interrupción afecta al área donde se encuentra el domicilio que figura en el contrato y el operador, a través de sus sistemas de información, no puede situarle en otra zona durante el período de la interrupción.

c) El abonado comunica al operador, mediante declaración responsable, en el plazo de 10 días contados a partir del restablecimiento del servicio, que ha estado en la zona afectada por la interrupción en el momento de producirse y dicha afirmación no resulta contradictoria con la obtenida de los sistemas de información del operador, circunstancia esta última que será debidamente comunicada por el operador al abonado.

En todo caso, la información a la que hacen referencia los supuestos anteriores, no podrá implicar el tratamiento de datos de localización.

Artículo 18. *Responsabilidad por daños.*

1. Los operadores responderán por los daños causados a los usuarios finales conforme a lo previsto en la legislación civil o mercantil y, en su caso, en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

2. La responsabilidad prevista en este artículo es distinta e independiente de la prevista en los artículos precedentes.

Artículo 19. *Suspensión temporal por impago del servicio telefónico desde una ubicación fija.*

1. El retraso en el pago total o parcial por el abonado durante un período superior a un mes desde la presentación a éste del documento de cargo correspondiente a la facturación del servicio telefónico disponible al público desde una ubicación fija podrá dar lugar, previo aviso al abonado, a su suspensión temporal. El impago del cargo por los servicios de acceso a Internet o de servicios de tarifas superiores, en especial del servicio de tarificación adicional, sólo dará lugar a la suspensión de tales servicios.

En caso de reclamación, corresponderá al operador probar que ha realizado el aviso previo a la suspensión a que se refiere el párrafo anterior.

2. En el supuesto de suspensión temporal del servicio telefónico por impago, éste deberá ser mantenido para todas las llamadas entrantes, excepto las de cobro revertido, y las llamadas salientes de urgencias.

3. El abonado tiene derecho a solicitar y obtener gratuitamente del operador del servicio la suspensión temporal de éste por un período determinado que no será menor de un mes ni superior a tres meses. El período no podrá exceder, en ningún caso, de 90 días por año natural. En caso de suspensión, se deducirá de la cuota de abono la mitad del importe proporcional correspondiente al tiempo al que afecte.

Artículo 20. *Interrupción definitiva por impago del servicio telefónico desde una ubicación fija.*

1. El retraso en el pago del servicio telefónico disponible al público desde una ubicación fija por un período superior a tres meses o la suspensión temporal, en dos ocasiones, del contrato por mora en el pago de los servicios correspondientes dará derecho al operador,

previo aviso al abonado, a la interrupción definitiva del servicio y a la correspondiente resolución del contrato. El impago del cargo por los servicios de acceso a Internet o de servicios de tarifas superiores, en especial del servicio de tarificación adicional, sólo dará lugar a la interrupción de tales servicios

2. Las condiciones en que puede efectuarse la suspensión o interrupción del servicio en los supuestos previstos tanto en este artículo como en el anterior serán fijados por orden ministerial. En la misma orden se regulará el procedimiento a seguir para la suspensión o interrupción.

CAPÍTULO VI

Derecho a la facturación desglosada, a la desconexión de determinados servicios y a elegir el medio de pago de los servicios entre los comúnmente utilizados en el tráfico comercial

Artículo 21. *Facturación de los servicios de comunicaciones electrónicas.*

Los usuarios finales tendrán derecho a que los operadores les presenten facturas por los cargos en que hayan incurrido. Las facturas deben contener de forma obligatoria y debidamente diferenciados los conceptos de precios que se tarifican por los servicios que se prestan. Los abonados a modalidades prepago tendrán derecho a obtener una información equivalente.

Los usuarios finales del servicio telefónico tendrán derecho a obtener facturación detallada, con el desglose que se establece en el artículo siguiente, sin perjuicio del derecho de los abonados a no recibir facturas desglosadas, al que se refiere el artículo 66 del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril.

Artículo 22. *Facturación desglosada del servicio telefónico.*

1. De acuerdo con lo establecido en el artículo anterior, los usuarios finales tendrán derecho a que los operadores del servicio telefónico disponible al público les presenten facturas por los cargos en que hayan incurrido, diferenciando debidamente los conceptos de precios que se tarifican por los servicios que se prestan, e incluso, previa solicitud, a que les presenten facturas independientes para los servicios de tarificación adicional.

2. Asimismo, los usuarios finales del servicio telefónico disponible al público tendrán derecho a obtener facturación detallada, sin perjuicio del derecho de los abonados a no recibir facturas desglosadas, con el nivel básico de detalle definido como el que incluye la identificación separada de los siguientes elementos:

a) El período de facturación.
b) La cuota mensual fija.
c) Otros cargos mensuales fijos.
d) Cualquier cuota fija no recurrente.
e) Detalle de todas las comunicaciones facturadas, excluidas las comunicaciones encuadradas en grupos tarifarios de bajo precio, tales como las metropolitanas, las de tarifa en horario normal inferior al equivalente de 3 céntimos de euro por minuto o a las de tarifa en horario normal inferior a 20 céntimos de euro por comunicación. Este detalle debe incluir: el número llamado, la fecha y hora de la llamada, la duración de la llamada, la tarifa aplicada y el coste total de la llamada. Las llamadas que tengan carácter gratuito para el abonado que efectúa la llamada no figurarán en la factura detallada de dicho abonado.
f) Datos agregados por grupos tarifarios diferenciados, tales como: metropolitanas, nacionales, internacionales, a móviles y tarificación adicional, que incluyan el número de llamadas efectuadas, el número total de minutos y el coste total de cada grupo.
g) Base imponible.
h) Total IVA o impuesto equivalente que le sea de aplicación.
i) Importe total de la factura, impuestos incluidos.

Los abonados a modalidades prepago tendrán derecho a tener acceso a una información equivalente, a través de los medios que se especifiquen en las correspondientes condiciones generales.

3. De acuerdo con lo establecido en el artículo 35.2.e) del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, el nivel básico de detalle de las facturas del servicio telefónico disponible al público será ofrecido de forma gratuita por el operador que lo preste como obligación de servicio universal.

En los demás casos, cuando los operadores no ofrezcan con carácter gratuito dicho nivel básico de detalle, y también en relación con la información sobre los consumos realizados para los abonados de prepago, o para desgloses más detallados que los indicados en el apartado anterior, los operadores deberán especificar su precio dentro de las condiciones de prestación del servicio. No obstante, cuando una factura o una cuenta prepago sea objeto de reclamación, de acuerdo con el procedimiento establecido en el artículo 27 de este real decreto, el operador deberá facilitar gratuitamente, previa solicitud del abonado, el nivel básico de detalle de la factura o cuenta reclamada.

4. El desglose establecido en este artículo se entiende, sin perjuicio de los establecidos en los apartados octavo y undécimo de la Orden PRE/361/2002, de 14 de febrero, de desarrollo, en lo relativo a los derechos de los usuarios y a los servicios de tarificación adicional, del título IV del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones.

Artículo 23. *Integración de otros cargos en la factura de los servicios de comunicaciones electrónicas.*

1. En el supuesto de que en la factura de un servicio de comunicaciones electrónicas se incluyan importes correspondientes a servicios que no tienen tal naturaleza, será obligatorio que se efectúe el desglose, de manera que pueda identificarse el importe correspondiente al servicio o servicios de comunicaciones electrónicas.

El usuario final que pague la parte de la factura que corresponda, según el desglose establecido en el párrafo anterior, al servicio de comunicaciones electrónicas no podrá ser suspendido en el mismo, sin perjuicio de la deuda que pueda subsistir por el importe impagado en otros conceptos. A estos efectos, en caso de disconformidad con la factura, el abonado tendrá derecho, previa petición, a la obtención de facturas independientes para cada servicio.

El incumplimiento de lo dispuesto en el párrafo primero de este artículo facultará al usuario final a considerar que la totalidad de la factura se libra por servicios que no tienen la consideración de comunicaciones electrónicas, por lo que su impago no podrá acarrear su suspensión.

2. Los usuarios finales tendrán derecho a obtener, a su solicitud, facturas independientes para los servicios de tarificación adicional y otros servicios de tarifas superiores y a las garantías sobre estos servicios que se establezcan por orden ministerial.

3. Los abonados a modalidades prepago tendrán derecho a la información desglosada y a las garantías establecidas en este artículo.

Artículo 24. *Derecho de desconexión de determinados servicios.*

1. Los operadores que presten el servicio telefónico disponible al público deberán garantizar a sus abonados el derecho a la desconexión de determinados servicios, entre los que se incluirá, al menos, el de llamadas internacionales y a servicios de tarificación adicional.

2. Los operadores que presten el servicio telefónico disponible al público regularán en sus correspondientes contratos de abono la forma de ejercicio del derecho de desconexión. A estos efectos, el abonado comunicará al operador, su intención de desconectarse de determinados servicios, debiendo admitirse en todo caso la petición escrita, y las realizadas por vía telefónica o telemática. El operador habrá de proceder a dicha desconexión como máximo en el plazo de 10 días desde la recepción de la comunicación del abonado. En caso de que dicha desconexión no se produjera tras esos 10 días, por causas no imputables al abonado, serán de cargo del operador los costes derivados del servicio cuya desconexión se solicita.

3. Las facturas o documentos de cargo que se emitan por los operadores que presten el servicio telefónico disponible al público para el cobro de los servicios prestados deberán reflejar, al menos semestralmente y de manera adecuada para ser percibido claramente por

el abonado, el derecho de desconexión establecido en este artículo. Los términos y la periodicidad en que dicha obligación deberá ser llevada a cabo podrán ser concretados mediante resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, previo informe del Instituto Nacional del Consumo y, en el caso de los servicios de tarificación adicional, de la Comisión de supervisión de servicios de tarificación adicional.

4. De acuerdo con lo establecido en el artículo 35.2.c) del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, la desconexión de los servicios previstos en el apartado 1 será ofrecida de forma gratuita por el operador que la preste como obligación de servicio universal.

Artículo 25. *Medios de pago.*

Los abonados tendrán derecho a la elección del medio de pago entre los comúnmente utilizados en el tráfico comercial. El contrato celebrado entre el operador y el usuario final deberá reflejar este derecho.

CAPÍTULO VII

Derecho a una atención eficaz por el operador

Artículo 26. *Servicio de atención al cliente de los operadores.*

1. Los operadores deberán disponer de un departamento o servicio especializado de atención al cliente, que tenga por objeto atender y resolver las quejas y reclamaciones y cualquier incidencia contractual que planteen sus clientes. Los titulares del departamento o servicio de atención al cliente serán los encargados de relacionarse, en su caso, con el servicio administrativo de solución de controversias a que se refiere el artículo 27 y al que remitirán la información que les sea requerida, con indicación del número de referencia asignado a la correspondiente reclamación.

No obstante lo dispuesto en el párrafo anterior, mediante orden ministerial podrá establecerse, en función del número de trabajadores del operador o de su volumen de negocio, la exención de la obligación de disponer del departamento o servicio especializado a que dicho párrafo se refiere, sin perjuicio del cumplimiento del resto de requisitos establecidos en el artículo 8.1.l).

2. El servicio de atención al cliente del operador, de carácter gratuito, deberá prestarse de manera tal que el usuario final tenga constancia de las reclamaciones, quejas y, en general, de todas las gestiones con incidencia contractual que realice el abonado. A dichos efectos, el operador estará obligado a comunicar al abonado el número de referencia de las reclamaciones, quejas, peticiones o gestiones. El operador deberá admitir, en todo caso la vía telefónica para la presentación de reclamaciones.

Si el medio habilitado por el operador para la atención de reclamaciones, incidencias o gestiones con incidencia contractual es telefónico, éste estará obligado a informar al consumidor de su derecho a solicitar un documento que acredite la presentación y contenido de la reclamación, incidencia o gestión mediante cualquier soporte que permita tal acreditación.

3. En caso de contratación telefónica o electrónica, si el usuario final se acoge a una oferta que prevea la aplicación de condiciones distintas a las condiciones generales publicadas conforme al artículo 12.1, el operador deberá enviarle, en el plazo de 15 días desde que se produzca la contratación, un documento en el que se expresen los términos y condiciones de la oferta, con indicación expresa de su plazo de duración.

4. El servicio de atención al cliente será accesible a los usuarios con discapacidad, según lo establecido en el artículo 3 del Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por Real Decreto 1494/2007, de 12 de noviembre, conforme a los plazos y condiciones establecidos en el mismo.

5. Las obligaciones que para los operadores se establecen en los apartados anteriores se entienden sin perjuicio de lo dispuesto en la legislación estatal y autonómica sobre protección general de consumidores y usuarios.

CAPÍTULO VIII

Derecho a vías rápidas y eficaces para reclamar

Artículo 27. *Controversias entre operadores y usuarios finales.*

1. Sin perjuicio de los procedimientos de mediación o resolución de controversias que, en su caso, hayan establecido los órganos competentes en materia de consumo de las Comunidades Autónomas, los abonados podrán dirigir su reclamación a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

2. El procedimiento de resolución de controversias ante la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, así como su ámbito de aplicación y requisitos, se regulará mediante orden del Ministro de Industria, Turismo y Comercio. El plazo para resolver y notificar la resolución será de seis meses.

3. El Ministerio de Industria, Turismo y Comercio podrá autorizar la ampliación de los plazos para la suspensión o la interrupción del servicio, previa solicitud de cualquier abonado que haya iniciado el procedimiento de resolución de conflictos al que se refiere el apartado anterior.

CAPÍTULO IX

Derecho a prestaciones especiales para personas con discapacidad y de renta baja

Artículo 28. *Medidas para garantizar la accesibilidad al servicio por las personas con discapacidad.*

1. De acuerdo con lo dispuesto en el artículo 22.1.d) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los operadores designados para la prestación del servicio universal deberán garantizar que los usuarios finales con discapacidad tengan acceso al servicio telefónico disponible al público desde una ubicación fija en condiciones equiparables a las que se ofrecen al resto de usuarios finales.

Dentro del colectivo de las personas con discapacidad, se considerarán incluidas las personas invidentes o con graves dificultades visuales, las personas sordas o con graves dificultades auditivas, las mudas o con graves dificultades para el habla, las minusválidas físicas y, en general, cualesquiera otras con discapacidades físicas que les impidan manifiestamente el acceso normal al servicio telefónico fijo o le exijan un uso más oneroso de este.

A los efectos de lo dispuesto en el apartado anterior, el operador designado garantizará la existencia de una oferta suficiente y tecnológicamente actualizada de terminales especiales, adaptados a los diferentes tipos de discapacidades, tales como teléfonos de texto, videoteléfonos o teléfonos con amplificación para personas con discapacidad auditiva, o soluciones para que las personas con discapacidad visual puedan acceder a los contenidos de las pantallas de los terminales, y realizará una difusión suficiente de aquélla.

El operador designado presentará, para su aprobación por el Ministerio de Industria, Turismo y Comercio, planes de adaptación de los teléfonos públicos de pago para facilitar su accesibilidad por los usuarios con discapacidad y, en particular, por los usuarios ciegos, en silla de ruedas o de talla baja.

El operador designado para la prestación del servicio universal, deberá ofrecer acceso a las guías telefónicas a través de Internet, en formato accesible para usuarios con discapacidad, en las condiciones y plazos de accesibilidad establecidos para las páginas de Internet de las administraciones públicas en el reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

Las obligaciones establecidas en este apartado se llevarán a cabo en las condiciones establecidas en el capítulo II del título III, del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril.

2. Los operadores deberán facilitar a los abonados con discapacidad visual que lo soliciten, en condiciones y formatos accesibles, los contratos, facturas y demás información suministrada a todos los abonados en cumplimiento de lo dispuesto en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y su normativa de desarrollo en materia de derechos de los usuarios. Cuando la información o comunicación se realice a través de Internet, será de aplicación lo dispuesto en el reglamento aprobado por el Real Decreto 1494/2007, de 12 de noviembre, para las páginas de las Administraciones Públicas o con financiación pública. Lo dispuesto en este párrafo se llevará a cabo en los términos establecidos en dicho real decreto.

Artículo 29. *Garantía del carácter asequible del servicio universal.*

El operador designado para la prestación del servicio universal deberá ofrecer a sus abonados, en las condiciones establecidas en el capítulo II del título III del reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, programas de precios de acceso y uso de los servicios incluidos en el servicio universal que permitan el máximo control del gasto por parte del usuario final y, en particular, los siguientes:

a) Abono social. Este plan de precios estará destinado a jubilados y pensionistas cuya renta familiar no exceda del indicador que se determine, en cada momento, por la Comisión Delegada del Gobierno para Asuntos Económicos, y consistirá en la aplicación de una bonificación en el importe de la cuota de alta y en la cuota fija de carácter periódico.

b) Usuarios invidentes o con grave discapacidad visual. Este plan consistirá en la aplicación de una determinada franquicia en las llamadas al servicio de consulta telefónica sobre números de abonado y en el establecimiento de las condiciones para la recepción gratuita de las facturas y de la publicidad de información suministrada a los demás abonados de telefonía fija sobre las condiciones de prestación de los servicios, en sistema Braille o en letras o caracteres ampliados, sin menoscabo de la oferta que de esta información se pueda realizar en otros sistemas o formatos alternativos.

c) Usuarios sordos o con graves dificultades auditivas. Este plan especial de precios se aplicará a las llamadas realizadas desde cualquier punto del territorio nacional que tengan como origen o destino un terminal de telefonía de texto, y que se establezcan a través del centro de servicios de intermediación para teléfonos de texto.

CAPÍTULO X

Protección en la utilización de servicios de tarificación adicional

Artículo 30. *Servicios de tarificación adicional.*

1. A los efectos de este real decreto, tendrán la consideración de servicios de tarificación adicional los que hayan sido declarados como tales por resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, en razón de la existencia de una facturación superior al coste del servicio de comunicaciones electrónicas y en interés de una especial protección de los derechos de los usuarios.

2. Mediante orden del Ministro de la Presidencia, a propuesta de los Ministros de Industria, Turismo y Comercio y de Sanidad y Política Social, se regulará la prestación de los servicios de tarificación adicional, su sujeción a un código de conducta, así como la composición y funcionamiento de la Comisión de supervisión de los servicios de tarificación adicional.

3. La prestación de servicios a los que acceda a través de la marcación de números telefónicos, y cuyos cargos figuren en la misma factura que los correspondientes a éstas, sólo podrá realizarse a través de códigos numéricos que hayan sido atribuidos para la prestación de servicios de tarificación adicional.

CAPÍTULO XI

Derecho a la protección de los datos personales

Artículo 31. *Derechos en materia de protección de datos.*

En relación con los datos personales, los usuarios finales serán titulares de los siguientes derechos:

a) Protección de datos personales sobre el tráfico.
b) Protección de datos en la facturación desglosada.
c) Protección de datos en la elaboración de guías telefónicas y de otros servicios de telecomunicaciones.
d) Protección de datos en la prestación de servicios de consulta sobre números de teléfono.
e) Protección frente a llamadas no solicitadas con fines comerciales.
f) Protección frente a la utilización de datos de localización.
g) Protección de datos personales en la prestación de servicios avanzados de telefonía.

La protección de datos personales en los servicios de comunicaciones electrónicas se regirá por la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, por el título V del Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril y, en lo no previsto por dichas normas, por lo dispuesto en la legislación vigente sobre protección de datos de carácter personal.

CAPÍTULO XII

Obligaciones de los usuarios finales

Artículo 32. *Obligaciones de los usuarios finales.*

Los usuarios finales de servicios de comunicaciones electrónicas, en sus relaciones con los operadores, deberán cumplir las siguientes obligaciones:

a) Contraprestación económica por el suministro del servicio y cumplimiento del resto de condiciones contractuales.
El usuario final tendrá la obligación de entregar al operador la contraprestación económica pactada en el contrato cuando haya recibido la prestación en los términos previstos en el mismo. La ausencia de tal contraprestación conllevará las consecuencias previstas en el propio contrato, sin perjuicio de las condiciones y requisitos establecidos en los artículos 19 y 20 de este real decreto.
Los usuarios finales estarán asimismo obligados al cumplimiento del resto de condiciones que figuren válidamente en los contratos que celebren con los operadores.
b) Uso del servicio para los fines previstos en el contrato.
Para ser titulares de los derechos reconocidos a los usuarios finales en este reglamento será precisa la utilización del servicio de comunicaciones electrónicas con los fines establecidos en el contrato. En particular, los usuarios que actúen como revendedores del servicio no serán titulares de los derechos reconocidos en este reglamento, sin perjuicio de los que le puedan corresponder en virtud del contrato y del resto de normativa aplicable.
c) Utilización de aparatos autorizados.
Los usuarios finales deberán utilizar equipos y aparatos cuya conformidad haya sido evaluada según la normativa vigente sobre evaluación de la conformidad de aparatos de telecomunicaciones.
d) Configuración de equipos y mantenimiento de la red más allá del punto de terminación de red.
Para una correcta recepción del servicio de comunicaciones electrónicas, será responsabilidad del abonado la correcta configuración de los equipos y aparatos, así como el mantenimiento de los elementos de red que, por situarse en un lugar posterior al punto de terminación de red, correspondan al usuario final, salvo que se haya previsto otra cosa en el contrato.
e) Suministro de datos personales exigidos por la legislación vigente.

Los usuarios finales deberán suministrar al operador los datos personales precisos a efectos de la obligación de identificación en la contratación de servicios de telefonía móvil prepago establecidos en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Disposición transitoria primera. *Vigencia de normas.*

Continuarán vigentes hasta que, en cumplimiento de lo dispuesto en este real decreto, sean sustituidas por otras, las siguientes normas:

a) La Orden PRE/361/2002, de 14 de febrero, de desarrollo, en lo relativo a los derechos de los usuarios y a los servicios de tarificación adicional, del título IV del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones.

b) La Orden ITC/912/2006, de 29 de marzo, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas

c) La Orden ITC/1030/2007, de 12 de abril, por la que se regula el procedimiento de resolución de las reclamaciones por controversias entre usuarios finales y operadores de servicios de comunicaciones electrónicas y la atención al cliente por los operadores.

d) La Orden ITC/308/2008, de 31 de enero, por la que se dictan instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia.

Disposición transitoria segunda. *Especificaciones de la portabilidad.*

La Comisión del Mercado de las Telecomunicaciones llevará a cabo las modificaciones necesarias en las especificaciones reguladoras de los procesos de conservación del número para la aplicación del plazo previsto en el artículo 44.3 del Reglamento aprobado por el Real Decreto 2296/2004, de 10 de diciembre, en su redacción dada por este real decreto. Una vez aprobadas, y en los términos previstos en ellas, será exigible el cumplimiento de dicho plazo.

Disposición transitoria tercera. *Códigos para la prestación de servicios de tarificación adicional.*

Lo dispuesto en el apartado 3 del artículo 30 sólo será exigible a partir de la entrada en vigor de la orden ministerial que se apruebe en cumplimiento del apartado 2 de dicho artículo.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogado el Título VI del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o menor rango se opongan a lo establecido en este real decreto.

Disposición final primera. *Modificación del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre.*

El primer párrafo del apartado 3 del artículo 44 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por el Real Decreto 2296/2004, de 10 de diciembre, queda redactado de la siguiente manera:

> «3. La conservación del número se efectuará en el plazo de 2 días hábiles contados desde el siguiente a la recepción de la solicitud de baja con conservación de número. No obstante lo anterior, la implementación técnica de la portabilidad deberá ser suficientemente flexible para poder acomodar futuras reducciones de los plazos de ejecución efectiva de la portabilidad, de conformidad con la legislación vigente, con el objetivo de llegar a realizarla en 24 horas.»

Disposición final segunda. *Título competencial.*

Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.21.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Incorporación de derecho de la Unión Europea.*

Mediante este real decreto se incorpora al derecho español la Directiva 2002/22/CE, del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

Disposición final cuarta. *Facultades de desarrollo.*

Se autoriza al Ministro de Industria, Turismo y Comercio a dictar las disposiciones necesarias para el desarrollo y aplicación de este real decreto.

Disposición final quinta. *Entrada en vigor.*

Este real decreto entrará en vigor a los tres meses de su publicación en el «Boletín Oficial del Estado».

§ 44

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. [Inclusión parcial]

Ministerio de la Presidencia
«BOE» núm. 287, de 30 de noviembre de 2007
Última modificación: 28 de abril de 2021
Referencia: BOE-A-2007-20555

[. . .]

LIBRO PRIMERO

Disposiciones generales

TÍTULO I

Ámbito de aplicación y derechos básicos de los consumidores y usuarios

[. . .]

CAPÍTULO II

Derechos básicos de los consumidores y usuarios

Artículo 8. *Derechos básicos de los consumidores y usuarios.*

1. Son derechos básicos de los consumidores y usuarios y de las personas consumidoras vulnerables:

a) La protección contra los riesgos que puedan afectar su salud o seguridad.
b) La protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos.
c) La indemnización de los daños y la reparación de los perjuicios sufridos.
d) La información correcta sobre los diferentes bienes o servicios y la educación y divulgación para facilitar el conocimiento sobre su adecuado uso, consumo o disfrute.
e) La audiencia en consulta, la participación en el procedimiento de elaboración de las disposiciones generales que les afectan directamente y la representación de sus intereses, a través de las asociaciones, agrupaciones, federaciones o confederaciones de consumidores y usuarios legalmente constituidas.

f) La protección de sus derechos mediante procedimientos eficaces, en especial en relación con las personas consumidoras vulnerables.

2. Los derechos de las personas consumidoras vulnerables gozarán de una especial atención, que será recogida reglamentariamente y por la normativa sectorial que resulte de aplicación en cada caso. Los poderes públicos promocionarán políticas y actuaciones tendentes a garantizar sus derechos en condiciones de igualdad, con arreglo a la concreta situación de vulnerabilidad en la que se encuentren, tratando de evitar, en cualquier caso, trámites que puedan dificultar el ejercicio de los mismos.

[. . .]

TÍTULO III

Contratos celebrados a distancia y contratos celebrados fuera del establecimiento mercantil

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 94. *Comunicaciones comerciales y contratación electrónica.*

En las comunicaciones comerciales por correo electrónico u otros medios de comunicación electrónica y en la contratación a distancia de bienes o servicios por medios electrónicos, se aplicará además de lo dispuesto en este título, la normativa específica sobre servicios de la sociedad de la información y comercio electrónico.

Cuando lo dispuesto en este título entre en contradicción con el contenido de la normativa específica sobre servicios de la sociedad de la información y comercio electrónico, ésta será de aplicación preferente, salvo lo previsto en el artículo 97.7, párrafo segundo.

[. . .]

Artículo 96. *Comunicaciones comerciales a distancia.*

1. En todas las comunicaciones comerciales a distancia deberá constar inequívocamente su carácter comercial.

2. En el caso de comunicaciones telefónicas, deberá precisarse explícita y claramente, al inicio de cualquier conversación con el consumidor y usuario, la identidad del empresario, o si procede, la identidad de la persona por cuenta de la cual efectúa la llamada, así como indicar la finalidad comercial de la misma. En ningún caso, las llamadas telefónicas se efectuarán antes de las 9 horas ni más tarde de las 21 horas ni festivos o fines de semana.

3. La utilización por parte del empresario de técnicas de comunicación que consistan en un sistema automatizado de llamadas sin intervención humana o el telefax necesitará el consentimiento expreso previo del consumidor y usuario.

El consumidor y usuario tendrá derecho a no recibir, sin su consentimiento, llamadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los referidos en el apartado anterior, cuando hubiera decidido no figurar en las guías de comunicaciones electrónicas disponibles al público, ejercido el derecho a que los datos que aparecen en ellas no sean utilizados con fines de publicidad o prospección comercial, o solicitado la incorporación a los ficheros comunes de exclusión de envío de comunicaciones comerciales regulados en la normativa de protección de datos personales.

4. El consumidor y usuario tendrá derecho a oponerse a recibir ofertas comerciales no deseadas, por teléfono, fax u otros medios de comunicación equivalente.

En el marco de una relación preexistente, el consumidor y usuario tendrá asimismo derecho a oponerse a recibir comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente. Debe ser informado en cada una de las comunicaciones comerciales de los medios sencillos y gratuitos para oponerse a recibirlas.

5. En aquellos casos en que una oferta comercial no deseada se realice por teléfono, las llamadas deberán llevarse a cabo desde un número de teléfono identificable. Cuando el usuario reciba la primera oferta comercial del emisor, deberá ser informado tanto de su derecho a manifestar su oposición a recibir nuevas ofertas como a obtener el número de referencia de dicha oposición. A solicitud del consumidor y usuario, el empresario estará obligado a facilitarle un justificante de haber manifestado su oposición que deberá remitirle en el plazo más breve posible y en todo caso en el plazo máximo de un mes.

El emisor estará obligado a conservar durante al menos un año los datos relativos a los usuarios que hayan ejercido su derecho a oponerse a recibir ofertas comerciales, junto con el número de referencia otorgado a cada uno de ellos, y deberá ponerlos a disposición de las autoridades competentes.

6. En todo caso, deberán cumplirse las disposiciones vigentes sobre protección de los menores y respeto a la intimidad. Cuando para la realización de comunicaciones comerciales se utilicen datos personales sin contar con el consentimiento del interesado, se proporcionará al destinatario la información que señala el artículo 30.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y se ofrecerá al destinatario la oportunidad de oponerse a la recepción de las mismas.

[. . .]

§ 45

Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios

Ministerio de Industria, Turismo y Comercio
«BOE» núm. 102, de 29 de abril de 2005
Última modificación: 29 de diciembre de 2018
Referencia: BOE-A-2005-6970

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, ha establecido un nuevo marco regulador de las telecomunicaciones en nuestro ordenamiento jurídico. Sus títulos II y III precisan de un desarrollo reglamentario que delimite el alcance de las obligaciones, tanto generales como de servicio público, que se imponen a los operadores. También es necesario concretar mediante norma reglamentaria otros aspectos, como la regulación del Registro de operadores, el procedimiento para la obtención de la condición de operador y los derechos de los usuarios.

En el apartado de la habilitación para la prestación de servicios y el establecimiento de redes de comunicaciones electrónicas, el reglamento recoge el régimen general de prestación de servicios y establecimiento y explotación de redes establecido por la ley. Toda vez que no existen títulos habilitantes individualizados para cada operador y servicio, se establece un repertorio de derechos y obligaciones que son de aplicación directa a los operadores, distinguiendo tanto entre operadores de redes y prestadores de servicios como entre prestadores del servicio telefónico y otros servicios.

En la regulación de las obligaciones de servicio público destaca el servicio universal, como conjunto de prestaciones que deben garantizarse a todos los usuarios finales, a precio asequible y con independencia de su localización en el territorio. Se concreta la determinación y el alcance de las prestaciones que incluye, se delimitan los procedimientos para la designación de los operadores encargados de garantizarlo y, finalmente, se establecen los criterios para la determinación de su coste y la imposición, si resulta preciso, de su mecanismo de financiación.

Se presta especial atención a la protección de los datos personales en la prestación de servicios de comunicaciones electrónicas. A este respecto, conviene señalar que esto se realiza a través de la regulación desde un triple punto de vista: el tratamiento de los datos que obren en poder de los operadores relativos al tráfico, facturación y localización de los abonados y usuarios, la elaboración de las guías telefónicas de números de abonados y la prestación de servicios avanzados de telefonía, como la identificación de la línea de origen, y el desvío automático de llamadas.

Este reglamento, al igual que la ley, garantiza el secreto de las comunicaciones. En él se incorpora el procedimiento para las interceptaciones legales de las comunicaciones que, de acuerdo con lo previsto en el artículo 579 de la Ley de Enjuiciamiento Criminal en la Ley

Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, y otras normas con rango de ley orgánica, pueda ordenar la autoridad judicial. Se establecen los requisitos técnicos y operacionales para que tales requerimientos judiciales sean convenientemente atendidos por los operadores de comunicaciones electrónicas.

Se regulan, además, los demás derechos de los usuarios de servicios de comunicaciones electrónicas, en aspectos tales como el contenido de los contratos entre los usuarios finales y los operadores, el derecho de desconexión de determinados servicios, el derecho a indemnización por la interrupción del servicio o el procedimiento de suspensión o interrupción de aquél ante situaciones de impago por los abonados.

Si bien el contenido principal del reglamento es, como se indica, el desarrollo del título III y del capítulo I del título II, ha resultado preciso realizar ciertas modificaciones en normas vigentes reguladoras de las comunicaciones electrónicas y las telecomunicaciones. Así, se modifica el Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, relativo al uso del dominio público radioeléctrico, aprobado por la Orden del Ministro de Fomento, de 9 de marzo de 2000, con el objetivo de adecuar su contenido al de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en especial en aspectos relativos a competencias y procedimientos.

Otra norma en la que se han introducido modificaciones es el Real Decreto 1029/2002, de 4 de octubre, por el que se establecen la composición y el régimen de funcionamiento del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información. La desaparición de las autorizaciones generales y licencias individuales como títulos habilitantes individuales hace preciso corregir ciertas referencias en la composición del Consejo. Este motivo impone la necesidad de modificar, asimismo, el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado por el Real Decreto 1066/2001, de 28 de septiembre, en cuanto contiene referencias a dichos títulos.

El reglamento también aborda problemas que pueden suscitarse por la entrada en vigor de la regulación que contiene. Cabe citar, entre otros, la transición de los antiguos Registros de titulares de licencias individuales y autorizaciones generales al nuevo Registro de operadores, la designación del operador encargado y las prestaciones del servicio universal y el régimen de derechos de los usuarios.

Esta disposición, además, complementa la transposición de las Directivas comunitarias que conforman el marco regulador de las comunicaciones electrónicas, esto es, la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas; la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas; la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas; la Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión; la Directiva 2002/77/CE de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas, y, finalmente, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Este reglamento se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones, reconocida en el artículo 149.1.21.ª de la Constitución.

En su virtud, a propuesta del Ministro de Industria, Turismo y Comercio, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 15 de abril de 2005,

D I S P O N G O :

Artículo único. *Aprobación del Reglamento.*

Se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, que se inserta a continuación.

Disposición adicional única. *Transformación de títulos habilitantes para el uso del dominio público radioeléctrico.*

En aplicación de lo dispuesto en el apartado 2.c) de la disposición transitoria primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, quedan transformadas en autorización administrativa para el uso privativo del dominio público radioeléctrico las licencias individuales para autoprestación con concesión demanial aneja de dicho dominio, y se mantiene el plazo de duración para el cual fueron otorgadas. Los órganos competentes en gestión del espectro radioeléctrico procederán de oficio a efectuar las correspondientes anotaciones en los títulos y anularán la licencia en autoprestación.

Disposición transitoria primera. *Títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Los procedimientos para el otorgamiento de derechos de uso del dominio público radioeléctrico iniciados antes de la entrada en vigor de este real decreto continuarán su tramitación conforme a la normativa anterior, si bien, conforme al apartado 8 de la disposición transitoria primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, el título habilitante que, en su caso, se otorgue se corresponderá con los previstos en dicha ley y en el Reglamento aprobado por la Orden de 9 de marzo de 2000, en su redacción dada por la disposición final primera de este real decreto.

2. Hasta la efectiva constitución de la Agencia Estatal de Radiocomunicaciones, la competencia para la tramitación y resolución de los procedimientos relativos a la gestión del dominio público radioeléctrico continuará correspondiendo a los órganos del Ministerio de Industria, Turismo y Comercio que la tenían atribuida hasta la entrada en vigor de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

3. Las concesiones para el uso privativo del dominio público radioeléctrico otorgadas antes de la entrada en vigor de este reglamento anejas a una licencia individual para la prestación de servicios a terceros se considerarán independientes de la habilitación de la persona titular de la citada concesión demanial para la prestación del servicio o la explotación de la red de comunicaciones electrónicas, y se mantendrá el plazo de validez para el cual fueron otorgados.

Disposición transitoria segunda. *Modelos de solicitud contenidos en el anexo III de la Orden de 22 de septiembre de 1998, por la que se establecen el régimen aplicable a las licencias individuales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares.*

Los modelos de solicitud contenidos en el anexo III de la Orden de 22 de septiembre de 1998, por la que se establecen el régimen aplicable a las licencias individuales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares, continuarán vigentes hasta que sean sustituidos por los que se aprueben mediante orden ministerial. Dichos modelos se entenderán referidos al título habilitante que corresponda para el uso del dominio público radioeléctrico.

Disposición transitoria tercera. *Composición del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.*

Mediante resolución del Presidente del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, se llevarán a cabo los nombramientos y ceses de vocales del Consejo para adaptar su composición a lo dispuesto en la disposición final segunda de este real decreto.

Hasta que se dicte la resolución a que se refiere el párrafo anterior, los vocales cuya representación desaparece conforme a lo establecido en la disposición final segunda continuarán como miembros del Consejo.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto y, en particular, las siguientes:

a) El Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones.

b) El Real Decreto 1652/1998, de 24 de julio, por el que se aprueba el Reglamento de los Registros especiales de titulares de licencias individuales y de titulares de autorizaciones generales para la explotación de servicios y para el establecimiento y explotación de redes de telecomunicaciones, y el Reglamento del procedimiento de ventanilla única para la presentación de solicitudes o notificaciones dirigidas a la obtención de dichos títulos.

c) La Orden de 22 de septiembre de 1998, por la que se establecen el régimen aplicable a las licencias individuales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares.

d) La Orden de 22 de septiembre de 1998, por la que se establecen el régimen aplicable a las autorizaciones generales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares.

e) La Orden de 21 de diciembre de 2001, por la que se regulan determinados aspectos del servicio universal de telecomunicaciones.

Disposición final primera. *Modificación del Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico.*

El Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico, aprobado por la Orden del Ministro de Fomento, de 9 de marzo de 2000, se modifica en los siguientes términos:

Uno. Los párrafos primero, cuarto y quinto del artículo 8 quedan redactados del siguiente modo:

> «Los interesados en obtener cualquier título habilitante para el uso del dominio público radioeléctrico presentarán sus solicitudes ante la Agencia Estatal de Radiocomunicaciones.»
>
> «La Agencia Estatal de Radiocomunicaciones, antes de dictar la resolución sobre el otorgamiento o denegación del título habilitante necesario para el uso del dominio público radioeléctrico y en el plazo previsto para ello, podrá requerir al solicitante cuanta información o aclaraciones considere convenientes sobre su solicitud o sobre los documentos con ella presentados. Las denegaciones de concesiones fundadas en la falta de acreditación de a condición de operador serán comunicadas a la Comisión del Mercado de las Telecomunicaciones.»
>
> «Cuando sea preciso para garantizar una gestión eficaz del espectro radioeléctrico, la Agencia Estatal de Radiocomunicaciones podrá modificar las características técnicas solicitadas previa audiencia del interesado y sin perjuicio del mantenimiento de los objetivos de servicio propuestos por el solicitante. En este supuesto, la validez del título otorgado estará condicionada a su aceptación por el solicitante.»

Dos. El artículo 9 queda redactado de la siguiente manera:

> **«Artículo 9.** *Plazos para resolver y notificar.*
>
> 1. El plazo para el otorgamiento y la notificación de las autorizaciones y concesiones de dominio público radioeléctrico será de seis semanas desde la

entrada de la solicitud en cualquiera de los registros del órgano competente. Dicho plazo podrá ser ampliado por el tiempo necesario para alcanzar la coordinación internacional de frecuencias o cuando afecte a reservas de posiciones orbitales.

2. No obstante lo dispuesto en el apartado anterior, cuando el título habilitante para el uso del dominio público radioeléctrico se otorgue mediante un procedimiento de licitación, el plazo máximo para resolver y notificar será de ocho meses desde la convocatoria de ésta.»

Tres. Se añade un inciso inicial al primer párrafo y se incorpora un párrafo quinto al artículo 14, con la siguiente redacción:

«El otorgamiento y duración de las autorizaciones para el uso especial del dominio público radioeléctrico, así como las condiciones exigibles a sus titulares, se establecerán mediante orden ministerial.»

«Las autorizaciones de uso especial tendrán carácter personal y conservarán su vigencia mientras su titular no manifieste su renuncia. No obstante, el titular deberá comunicar fehacientemente a la Administración cada cinco años, contados desde la fecha de otorgamiento de la autorización, su intención de continuar utilizando el dominio público radioeléctrico. El incumplimiento de este deber será causa de extinción de la autorización, previa tramitación del correspondiente expediente, cuyo procedimiento se establecerá mediante orden ministerial.»

Cuatro. El párrafo primero del artículo 17 queda redactado de la siguiente manera:

«Los titulares de las asignaciones de frecuencias deberán cumplir, además de las condiciones que les vengan impuestas en la resolución del título del uso del espectro radioeléctrico, las correspondientes al régimen de autorización general que resulten aplicables en la explotación de la red o la prestación del servicio.»

Cinco. El párrafo primero del artículo 19 queda redactado de la siguiente manera:

«Sin perjuicio de lo dispuesto en el artículo 37, la Agencia Estatal de Radiocomunicaciones resolverá, en los plazos que en cada caso procedan, de acuerdo con el artículo 9, sobre el otorgamiento de los títulos solicitados.»

Seis. El párrafo primero del artículo 20 queda redactado de la siguiente manera:

«La Agencia Estatal de Radiocomunicaciones podrá denegar las solicitudes por alguna de las siguientes causas:»

Siete. Los párrafos primero y segundo del artículo 21 quedan redactados del siguiente modo, y se añade un párrafo cuarto, con la siguiente redacción:

«Los títulos habilitantes que otorguen derechos de uso del dominio público radioeléctrico, citados en el artículo 18, tendrán el período de vigencia inicial que para cada uno de ellos se fija en los artículos siguientes. Dichos títulos habilitantes podrán ser objeto de sucesivas prórrogas.»

«La Agencia Estatal de Radiocomunicaciones podrá modificar, en cualquier momento, durante el período de vigencia de un título habilitante que otorgue derechos de uso privativo sobre el dominio público radioeléctrico, las características técnicas y las bandas de frecuencias asignadas cuando ello sea preciso para su adecuación al Cuadro nacional de atribución de frecuencias, por razones de uso eficiente del espectro radioeléctrico, de acuerdo con lo previsto en el artículo 11, o por obligaciones derivadas del cumplimiento de la normativa internacional o comunitaria.»

«Mediante orden ministerial, previa audiencia de los interesados, de las asociaciones de usuarios e informe de la Comisión del Mercado de las Telecomunicaciones, y con respeto a la legislación sobre patrimonio de las Administraciones públicas, se podrán modificar las condiciones generales a que se sujetan los títulos habilitantes para el uso privativo del dominio público radioeléctrico, con arreglo a los principios de objetividad y proporcionalidad, y atendiendo principalmente a las necesidades de la planificación y del uso eficiente y la disponibilidad del espectro radioeléctrico.»

Ocho. Los párrafos primero y segundo del artículo 23 quedan redactados de la siguiente manera:

«El incumplimiento de las condiciones y requisitos técnicos aplicables al uso del dominio público radioeléctrico podrá dar lugar a la revocación, por la Agencia Estatal de Radiocomunicaciones, del título habilitante que otorga derecho a su uso privativo, previa tramitación del correspondiente expediente, a través del procedimiento general de la Ley 30/1992, de 26 de noviembre.

Asimismo, la pérdida de la condición de operador del titular del derecho de uso del dominio público radioeléctrico, por alguna de las causas previstas en el capítulo I del título II del Reglamento relativo a las condiciones para la prestación de servicios o la explotación de redes de comunicaciones electrónicas, llevará aparejada la de las concesiones de uso privativo de dicho dominio.»

Nueve. El párrafo e) del artículo 24 queda redactado de la siguiente manera:

«e) Por la pérdida de la condición de operador del titular del derecho de uso del dominio público radioeléctrico, en caso de tratarse de concesiones de uso privativo, o cualquier causa que imposibilite la prestación del servicio por su titular.»

Diez. El artículo 25 queda redactado de la siguiente manera:

«Artículo 25. *Inspección previa al uso del espectro.*

De acuerdo con el artículo 45 de la Ley General de Telecomunicaciones, será requisito previo a la utilización del dominio público radioeléctrico la inspección o reconocimiento satisfactorio de las instalaciones por la Agencia Estatal de Radiocomunicaciones.

En función de la naturaleza del servicio, de la banda de frecuencias empleada, de la importancia técnica de las instalaciones que se utilicen o por razones de eficacia en la gestión del espectro, dicha inspección o reconocimiento previo podrá ser sustituida por una certificación expedida por técnico competente a la que se refiere el artículo 45.4 de la Ley General de Telecomunicaciones.

Mediante resolución del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, se podrán establecer bandas de frecuencias o servicios en los que, conforme al párrafo anterior, la inspección podrá ser sustituida por la certificación prevista en él.»

Once. El artículo 27 queda redactado de la siguiente manera:

«Artículo 27. *Presentación de solicitudes.*

Los interesados en obtener una afectación de dominio público radioeléctrico deberán dirigir una solicitud a la Agencia Estatal de Radiocomunicaciones, acompañada de una propuesta técnica en la que se defina con precisión la estructura y características técnicas de la red de comunicaciones que se pretende instalar y el servicio o servicios a los que se pretende destinar.»

Doce. El artículo 29 queda redactado de la siguiente manera:

«Artículo 29. *Plazo de vigencia.*

Las afectaciones de dominio público radioeléctrico se otorgarán por un período de tiempo máximo que finalizará el 31 de diciembre del año natural en que cumpla su quinto de vigencia, prorrogable, previa petición de su titular, por períodos de cinco años.»

Trece. El artículo 30 queda redactado de la siguiente manera:

«Artículo 30. *Derechos de uso privativo del dominio público radioeléctrico.*

El derecho de uso privativo de dominio público radioeléctrico por personas físicas o jurídicas, o por las Administraciones públicas y entes públicos de ellas dependientes, para fines distintos de los expresados en el artículo 26, se otorgará mediante a correspondiente autorización o concesión por la Agencia Estatal de Radiocomunicaciones.

Las concesiones y autorizaciones que otorguen derecho al uso privativo del dominio público radioeléctrico estarán sujetas a lo dispuesto en este reglamento. No obstante, a las concesiones otorgadas mediante un procedimiento de licitación les será de aplicación lo dispuesto en la orden ministerial que apruebe el correspondiente pliego de bases de la adjudicación y en este reglamento en lo que no se oponga a aquélla.»

Catorce. El artículo 31 queda redactado de la siguiente manera:

«Artículo 31. *Concesiones y autorizaciones para el uso privativo del dominio público radioeléctrico.*

El derecho al uso privativo del dominio público radioeléctrico distinto al regulado en el capítulo II de este título se obtendrá mediante concesión administrativa, en los términos establecidos en este capítulo. Para la obtención de una concesión demanial, el solicitante deberá acreditar su condición de operador.

No obstante lo dispuesto en el párrafo anterior, el derecho al uso del dominio público radioeléctrico se podrá adquirir mediante la obtención de la correspondiente autorización administrativa cuando la utilización de dicho dominio se realice en régimen de autoprestación, salvo en el caso de las Administraciones públicas, que requerirán afectación demanial.

Las concesiones para el uso privativo del dominio público radioeléctrico se otorgarán por un período inicial que finalizará el 31 de diciembre del año natural en que cumpla su quinto de vigencia, prorrogable, a petición del interesado, por períodos sucesivos de cinco años.

Sin perjuicio de lo dispuesto en el artículo 6, las concesiones demaniales serán accesibles al público mediante el acceso, a través de Internet, al Registro público de radiofrecuencias, que llevará la Agencia Estatal de Radiocomunicaciones, conforme al artículo 47 de la Ley General de Telecomunicaciones.

Una vez otorgada la concesión de uso del dominio público radioeléctrico, se notificará al particular, quien estará obligado al pago del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados, conforme a su normativa reguladora.

El titular de la concesión deberá acreditar, en el plazo de tres meses desde la notificación, el pago del impuesto a que se refiere el párrafo anterior. Una vez se produzca dicha acreditación, la concesión se inscribirá en el Registro público de radiofrecuencias en el plazo de 15 días. Transcurridos los tres meses sin que se haya producido la acreditación, la concesión será revocada mediante resolución del órgano competente para otorgarla conforme a lo establecido en el artículo 23.»

Quince. El primer párrafo del artículo 32 queda redactado de la siguiente manera:

«La transmisión del título habilitante para el uso del espectro requerirá la autorización del órgano administrativo que lo otorgó.»

Dieciséis. El primer párrafo del artículo 33 queda redactado de la siguiente manera, y se añade un párrafo tercero, con la siguiente redacción:

«La solicitud de autorización, junto a la propuesta técnica, se dirigirá a la Agencia Estatal de Radiocomunicaciones, en impreso formulario debidamente cumplimentado. Dicho impreso será aprobado por la Agencia Estatal de Radiocomunicaciones y publicado en el "Boletín Oficial del Estado".»

«No se otorgarán derechos de uso privativo del dominio público radioeléctrico para su uso en autoprestación en los supuestos en que la demanda supere a la oferta y se aplique el procedimiento de licitación previsto en el artículo 37.»

Diecisiete. Los dos primeros párrafos del artículo 34 quedan redactados del siguiente modo, y se sustituye en el tercer párrafo la expresión «El Ministerio de Fomento podrá:» por «La Agencia Estatal de Radiocomunicaciones podrá:»

«Toda autorización se otorgará por un período de tiempo inicial que finalizará el 31 de diciembre del año natural en que cumpla su quinto de vigencia, prorrogable por períodos sucesivos de cinco años.

Si el titular deseara prorrogar la autorización, deberá solicitarlo con tres meses de antelación a la finalización de su vigencia. Si al concluir el período de vigencia de la autorización la Administración no se hubiera pronunciado sobre la solicitud de prórroga, ésta se entenderá desestimada.»

Dieciocho. El artículo 35 queda derogado.

Diecinueve. La rúbrica de la sección 3.ª pasa a denominarse «Concesiones de dominio público radioeléctrico otorgadas mediante un procedimiento de licitación».

Veinte. El artículo 37 queda redactado de la siguiente manera:

«Artículo 37. *Limitación del número de concesiones por razón del uso eficaz del espectro radioeléctrico.*

1. Cuando sea preciso para garantizar el uso eficaz del espectro radioeléctrico, la Agencia Estatal de Radiocomunicaciones suspenderá el otorgamiento de concesiones y propondrá al Ministerio de Industria, Turismo y Comercio la limitación del número de concesiones demaniales que se otorguen sobre dicho dominio.

2. En el supuesto previsto en el apartado anterior, será de aplicación lo siguiente:

a) El Ministerio de Industria, Turismo y Comercio llevará a cabo un trámite de audiencia para conocer la posible existencia de interesados en la prestación del servicio o el establecimiento y explotación de la red. En dicho trámite se recabará la opinión, aparte de los interesados, del Consejo de Consumidores y Usuarios.

b) Tras el trámite anterior, el Ministerio de Industria, Turismo y Comercio adoptará, en su caso, la decisión de limitar el número de concesiones que se vayan a otorgar y suspenderá el otorgamiento de títulos habilitantes en el segmento de espectro afectado por dicha decisión.

c) Mediante orden ministerial, previo informe de la Comisión del Mercado de las Telecomunicaciones, se aprobará el pliego de bases y la convocatoria de un procedimiento de licitación para el otorgamiento de las concesiones. En el citado pliego deberá establecerse:

1.º La cantidad de espectro asociada, las características de su utilización, el plazo de vigencia de las concesiones, que no podrá exceder de 20 años prorrogables, o cualquier otra característica o condición para su uso efectivo.

2.º Los requisitos y condiciones que hayan de cumplir los licitadores y los posibles adjudicatarios, que deberán tener la condición de operador en el momento de finalización del plazo de presentación de licitaciones.

3.º El procedimiento de adjudicación, que podrá ser de concurso o subasta, y que respetará en todo caso los principios de publicidad, concurrencia y no discriminación.

4.º Las condiciones en que deba prestarse el servicio o explotarse la red de comunicaciones electrónicas a que esté destinado el dominio público radioeléctrico adjudicado.

d) En todo lo no previsto en el pliego de bases en relación con la convocatoria, adjudicación, modificación, transmisión y extinción de las concesiones otorgadas mediante este procedimiento, será de aplicación la legislación de contratos de las Administraciones públicas

e) El procedimiento de licitación deberá resolverse y notificarse en un plazo máximo de ocho meses desde la publicación de la convocatoria.

f) Las condiciones en que deba prestarse el servicio o explotarse la red mediante el uso del dominio público radioeléctrico adjudicado serán las previstas en la Ley General de Telecomunicaciones y su normativa de desarrollo, las específicas establecidas en el pliego de bases y las que el adjudicatario haya asumido en su propuesta.

3. La limitación del número de concesiones de dominio público radioeléctrico será revisable por el Ministerio de Industria, Turismo y Comercio, de oficio o a instancia de parte, en la medida en que desaparezcan las causas que la motivaron. En el caso de efectuarse dicha revisión, no habrá derecho a indemnización a favor de los operadores que hubieran obtenido sus concesiones mediante el procedimiento de licitación, sin perjuicio del derecho de dichos operadores a la cancelación de las

garantías que, en su caso, hubiesen constituido para responder de compromisos asumidos en el procedimiento.»

Veintiuno. Los artículos 38 y 39 quedan derogados.

Veintidós. El apartado 1 del artículo 40 queda redactado de la siguiente manera y se añade un inciso final al antepenúltimo párrafo, con la siguiente redacción:

«1. Cuando el procedimiento se inicie de oficio por la Administración, los recursos obtenidos podrán ser explotados en régimen de gestión directa o indirecta. En este último caso, la Agencia Estatal de Radiocomunicaciones propondrá al Ministerio de Industria, Turismo y Comercio la convocatoria del correspondiente concurso público. Todos los gastos derivados de este procedimiento se repercutirán al adjudicatario en el momento del otorgamiento del título habilitante.»

«No obstante, la constitución de esta garantía no será exigible si, al otorgarse recursos órbita-espectro adicionales a los ya poseídos por el titular, se encontrara vigente una garantía constituida por él afecta a obligaciones ya cumplidas.»

Veintitrés. El último párrafo del artículo 40 queda redactado de la siguiente manera y se añade un apartado 3, con la siguiente redacción:

«Una vez obtenido el recurso, el Ministerio de Industria, Turismo y Comercio otorgará mediante adjudicación directa al peticionario el correspondiente título habilitante, el cual tendrá vigencia, en caso de lanzamiento de un satélite, durante su vida útil, sin que en ningún caso pueda exceder de 30 años desde la adjudicación.»

«3. El derecho de uso del dominio público radioeléctrico sobre los recursos órbita-espectro en el ámbito de la soberanía española destinados a una misión gubernamental podrá ser cedido por su titular al tercero al que la Administración que tenga encomendada dicha misión designe. La cesión deberá ser aprobada por el Ministerio de Industria, Turismo y Comercio y se llevará a cabo en los términos fijados por éste, previo informe del titular de la misión gubernamental.

La cesión a que se refiere el párrafo anterior será gratuita, y tendrá vigencia por el plazo total del título habilitante de los recursos órbita-espectro o, alternativamente, por la vida útil de la misión gubernamental.»

Veinticuatro. El párrafo primero del artículo 42 queda redactado de la siguiente manera:

«La utilización del dominio público radioeléctrico para la instalación y explotación de redes de transporte de señales de los servicios de radiodifusión sonora y de televisión requerirá la correspondiente concesión otorgada por la Administración del Estado.»

Veinticinco. El artículo 43 queda derogado.

Veintiséis. El artículo 44 queda redactado de la siguiente manera:

«Artículo 44. *Concepto, títulos habilitantes y régimen jurídico.*

Tendrán la consideración de eventos de corta duración la realización de pruebas técnicas, los de cobertura de acontecimientos deportivos y, en general, cualquier utilización del dominio público radioeléctrico por un período breve de tiempo.

El régimen aplicable a las autorizaciones de dominio público radioeléctrico para eventos de corta duración será el establecido en el capítulo III de este título, con excepción de lo dispuesto en lo relativo a su duración, que será de un período máximo improrrogable de seis meses.»

Veintisiete. Se añade una disposición adicional cuarta, con la siguiente redacción:

«Disposición adicional cuarta. *Servicios en los que se limita el número de concesiones demaniales.*

De conformidad con lo previsto en el artículo 37, se consideran servicios en los que, por ser precisa la garantía del uso eficiente del dominio público radioeléctrico, se limita el número de concesiones para el uso de dicho dominio:

a) El servicio de telefonía móvil automática en su modalidad GSM.

b) El servicio de comunicaciones móviles personales en su modalidad DCS 1800.

c) El servicio de comunicaciones móviles de tercera generación UMTS.

d) El servicio de distribución de vídeo vía radio mediante el sistema SDVM (sistema de distribución de vídeo multipunto).

e) El servicio de comunicaciones móviles en grupos cerrados de usuarios con tecnología digital de ámbito nacional.»

Disposición final segunda. *Modificación del Real Decreto 1029/2002, de 4 de octubre, por el que se establece la composición y el régimen de funcionamiento del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.*

El Real Decreto 1029/2002, de 4 de octubre, por el que se establece la composición y el régimen de funcionamiento del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, se modifica en los siguientes términos:

Uno. El párrafo primero del artículo 1 queda redactado de la siguiente manera:

«El Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, previsto en la disposición adicional quinta de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, es un órgano asesor del Gobierno en materia de telecomunicaciones y Sociedad de la Información.»

Dos. El párrafo b) del artículo 2 queda redactado de la siguiente manera:

«b) Conocer e informar los proyectos legislativos y reglamentarios, en aplicación de la Ley 32/2003,de 3 de noviembre, General de Telecomunicaciones.»

Tres. El artículo 4 queda redactado de la siguiente manera:

«Artículo 4. *Vocales.*

1. Serán vocales del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información:

A) En representación de la Administración General del Estado:

a) Seis representantes del Ministerio de Industria, Turismo y Comercio, nombrados por el Presidente del Consejo, con categoría, al menos, de subdirector general o asimilado, de los que uno corresponderá necesariamente a la Dirección General de Telecomunicaciones y Tecnologías de la Información, otro a la Dirección General para el Desarrollo de la Sociedad de la Información, y otro será el Secretario del Consejo, que actuará, asimismo, como secretario de la Comisión Permanente.

b) Además, serán vocales del Consejo, nombrados por el Presidente, a propuesta de los titulares de los departamentos respectivos, con categoría, al menos, de subdirector general o asimilado, en su caso:

1.º Un representante de la Presidencia del Gobierno.

2.º Un representante de cada departamento ministerial y de los ministros previstos por el artículo 4.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno, si los hubiera.

3.º Un representante de la Comisión Superior de Informática y para el impulso de la Administración electrónica.

4.º Un representante de la Agencia Española de Protección de Datos.

B) En representación de las Administraciones autonómica y local, serán designados por el Presidente del Consejo:

a) Un representante de cada comunidad autónoma, propuesto por ésta.

b) Dos representantes de la Administración local, propuestos por la asociación de entidades locales de ámbito estatal con mayor implantación.

C) Por los industriales y comercializadores, designados por el Presidente del Consejo, a propuesta de las asociaciones empresariales del sector:

a) Dos representantes de la industria de fabricación de equipos de telecomunicación.

b) Un representante de los comercializadores e importadores de equipos de telecomunicación y de tecnologías de la información.

c) Dos representantes de las asociaciones de los instaladores de telecomunicación.

d) Dos representantes de la industria de fabricación de equipos y desarrollo de aplicaciones relacionados con la sociedad de la información.

D) Por los prestadores de servicios de telecomunicación, de difusión y de la sociedad de la información, designados por el Presidente del Consejo, a propuesta de las entidades, empresas, asociaciones o centros directivos correspondientes:

a) Por los prestadores de servicios de telecomunicaciones:

1.º Dos representantes por los operadores titulares de concesiones de dominio público radioeléctrico con limitación de número, otorgadas mediante un procedimiento de licitación.

2.º Un representante por cada entidad prestadora de las obligaciones de servicio público previstas en los artículos 22, 25.1 y 25.2.d) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

3.º Un representante de la asociación más representativa de los operadores no incluidos en el párrafo anterior.

4.º Un representante de la entidad prestadora de la obligación de servicio público prevista en el apartado 1 de la disposición transitoria cuarta del Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico, aprobado por la Orden de 9 de marzo de 2000.

b) Por los prestadores de servicios de difusión:

1.º Un representante de la entidad prestadora del servicio público esencial de televisión, regulado por la Ley 4/1980, de 10 de enero, del Estatuto de la Radio y la Televisión.

2.º Dos representantes de las entidades o sociedades prestadoras del servicio público esencial de televisión, regulado por la Ley 46/1983, de 26 de diciembre, reguladora del tercer canal de televisión.

3.º Un representante de cada una de las sociedades concesionarias del servicio de televisión privada analógica de ámbito nacional, regulado por la Ley 10/1988, de 3 de mayo.

4.º Un representante de las sociedades prestadoras del servicio de televisión por satélite.

5.º Dos representantes de las sociedades titulares del servicio de difusión de televisión por cable regulado en la Ley 42/1995, de 22 de diciembre.

6.º Dos representantes de las sociedades prestadoras del servicio de televisión digital por ondas terrestres de ámbito nacional, siempre que no gestionen otra modalidad del servicio de televisión.

7.º Dos representantes de las sociedades prestadores del servicio de televisión privada de ámbito autonómico y local.

8.º Tres representantes por los prestadores de servicios de radiodifusión sonora: uno, por el sector público estatal; otro, por el sector público autonómico, y un tercero, por el sector privado.

c) Por los prestadores de servicio de la sociedad de la información:

1.º Uno por los prestadores de servicios de certificación de firma electrónica de entre los que operan en la Administración.

2.º Uno por el resto de prestadores de servicios de certificación de firma electrónica.

3.º Uno por los prestadores de servicios de intermediación de la sociedad de la información.

4.º Uno por la asociación más representativa de ámbito nacional de las empresas prestadoras de servicios de comercio electrónico.

5.º Uno por la entidad gestora del registro de nombres de dominio de Internet bajo el código de país correspondiente a España (" .es").

E) Por los usuarios:

a) Dos representantes de las asociaciones de consumidores y usuarios, designados por el Presidente del Consejo, a propuesta del Consejo de Consumidores y Usuarios.

b) Un representante de las asociaciones de usuarios de servicios de telecomunicaciones, designado por el Presidente del Consejo, a propuesta de éstas.

c) Dos representantes de asociaciones representativas de usuarios de Internet, designados por el Presidente del Consejo, a propuesta de éstas.

d) Un representante de la asociación más representativa de los usuarios con discapacidad a los que debe ser garantizada la prestación del servicio universal, de conformidad con el artículo 22.1.d) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

F) Por los sindicatos, cuatro representantes de las organizaciones sindicales, designados por el Presidente del Consejo, a propuesta de éstas. El número de representantes de cada organización sindical será proporcional al de los representantes obtenidos en las elecciones sindicales, en el ámbito estatal, en el sector de las telecomunicaciones y de la sociedad de la información.

G) Por las corporaciones de derecho público en defensa de intereses profesionales o sectoriales, cuatro representantes:

a) Uno por el Colegio Oficial de Ingenieros de Telecomunicación y otro por el Colegio Oficial de Ingenieros Técnicos de Telecomunicación, designados por el Presidente, a propuesta de cada uno de ellos.

b) Uno por los colegios profesionales correspondientes a titulaciones de ingeniería no representados en el párrafo anterior, a propuesta de la Real Academia de Ingeniería.

c) Uno por el Consejo Superior de Cámaras de Comercio, Industria y Navegación de España, a su propuesta.

H) Hasta un máximo de cuatro vocales, designados por el Presidente del Consejo, entre personalidades de reconocido prestigio en el sector de las telecomunicaciones y de la sociedad de la información.

2. La representación de los vocales del Consejo Asesor en la Comisión Permanente de este órgano se efectuará conforme a lo establecido en el artículo 13.

3. La designación de los vocales, cuando se realice a propuesta de asociaciones o entidades, deberá ajustarse a la propuesta.»

Cuatro. El apartado 1 del artículo 13 queda redactado de la siguiente manera:

«1. La Comisión Permanente estará compuesta por los Vicepresidentes y los siguientes vocales:

a) Seis del grupo del apartado A) del artículo 4.1, de los que tres corresponderán al Ministerio de Industria, Turismo y Comercio; uno, al Ministerio de Defensa; uno, al Ministerio de Administraciones Públicas, y uno, al Ministerio de Economía y Hacienda. De los tres primeros, uno pertenecerá a la Dirección General de Telecomunicaciones y Tecnologías de la Información; otro, a la Dirección General para el Desarrollo de la Sociedad de la Información, y el tercero será el Secretario del Consejo, que actuará, asimismo, como secretario de la Comisión Permanente.

b) Dos del grupo del apartado B) del artículo 4.1, uno de los cuales corresponderá a las comunidades autónomas, propuesto por ellas, y otro a la Administración local, a su propuesta.

c) Dos del grupo del apartado C) del artículo 4.1, de los cuales uno corresponderá a la industria de fabricación de equipos de telecomunicación, y el otro, a los comercializadores e importadores de equipos de telecomunicación y de tecnologías de la información.

d) Cinco del grupo a) del apartado D) del artículo 4.1, distribuidos de la siguiente manera:

1.º Uno por cada prestador de las obligaciones de servicio público de los artículos 22, 25.1 y 25.2.d) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2.º Uno en representación de la asociación más representativa de los operadores no incluidos en el párrafo anterior.

3.º Uno en representación del prestador de la obligación de servicio público prevista en el apartado 1 de la disposición transitoria cuarta del Reglamento relativo al uso del dominio público radioeléctrico.

e) Cinco del grupo b) del apartado D) del artículo 4.1, distribuidos del siguiente modo:

1.º Un representante de los prestadores públicos estatales de los servicios de radiodifusión y televisión.

2.º Un representante de los prestadores públicos autonómicos de los servicios de radiodifusión y televisión.

3.º Dos representantes de los prestadores de servicios de televisión privada incluidos en los apartados 4.º, 5.º, 6.º y 7.º del grupo D.b) del artículo 4.1.

4.º Un representante del sector de la televisión privada analógica de ámbito nacional y del sector de la radiodifusión privada incluidos en los párrafos 3.º y 8.º del artículo 4.1.D).b).

f) Dos por el grupo c) del apartado D) del artículo 4.1, de los cuales uno corresponderá a la entidad gestora del registro de nombres de dominio de Internet bajo el código (" .es"), y otro, al resto de entidades integradas en dicho grupo.

g) Cuatro por el grupo del apartado E) del artículo 4.1, de los cuales corresponderá uno a cada uno de los grupos integrados en dicho apartado.

h) Uno al grupo del apartado F) del artículo 4.1.

i) Uno del grupo a) del apartado G), y otro del apartado H) del artículo 4.1.

Los vocales de cada uno de los grupos y subgrupos de los apartados del artículo 4 elegirán de entre sus miembros al vocal o vocales que deban formar parte de la Comisión Permanente.

El suplente de cada uno de los vocales y del Secretario de la Comisión Permanente será el mismo que tenga dicha condición respecto de los vocales y el Secretario del Pleno del Consejo Asesor, de acuerdo con lo establecido en el artículo 6.»

Cinco. El segundo párrafo del apartado 1 del artículo 14 queda redactado de la siguiente manera:

«Estas ponencias, que tendrán la consideración de grupos de trabajo del Consejo Asesor, estarán presididas por uno de los miembros del Consejo, designado por su Presidente, e integradas por aquellos que decida la Comisión Permanente. Podrán estar asistidas por personas vinculadas al sector de las telecomunicaciones y de la sociedad de la información o expertas en los asuntos que sean objeto de estudio por la ponencia, designadas por el presidente de ésta.»

Seis. Queda derogado el apartado 3 del artículo 14.

Disposición final tercera. *Modificación del Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones, aprobado por el Real Decreto 1890/2000, de 20 de noviembre.*

El Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones, aprobado por el Real Decreto 1890/2000, de 20 de noviembre, se modifica en los siguientes términos:

Uno. El artículo 10 queda redactado de la siguiente manera:

«Artículo 10. *Interfaces reglamentadas.*

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información publicará como resolución en el "Boletín Oficial del Estado" las interfaces reglamentadas en España que hayan sido notificadas a la Comisión Europea.»

Dos. El párrafo cuarto del artículo 21 queda redactado de la siguiente manera:

«Como consecuencia de la notificación recibida, se comunicará al interesado si procede la puesta en el mercado nacional y, en su caso, las restricciones de uso o limitaciones geográficas, para el uso del citado equipo.»

Tres. El apartado 3 del artículo 30 queda redactado de la siguiente manera:

«3. Si el fabricante, o su mandatario establecido en la Unión Europea o la persona responsable de la puesta en el mercado, desea evaluar la conformidad en virtud de lo dispuesto en este capítulo, presentará los documentos anteriormente

descritos ante un organismo notificado de la Unión Europea. En el caso de optar por la intervención de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información como organismo notificado, presentará el expediente técnico de construcción, acompañado de su manual de usuario, ante dicha Secretaría de Estado, y solicitará la emisión del informe técnico tras la revisión del expediente técnico de construcción, para lo que utilizará, de forma voluntaria, el modelo de solicitud establecido en el anexo III.1.»

Cuatro. Los apartados 5, 6 y 7 del artículo 30 quedan redactados de la siguiente manera:

«5. El organismo notificado español elegido revisará el expediente técnico de construcción para verificar si se cumple todo lo establecido en este reglamento y podrá emitir, en el plazo máximo de 28 días naturales a partir de la recepción del expediente, un dictamen que será enviado al fabricante del aparato, a su mandatario establecido en la Unión Europea, o a la persona responsable de la puesta en el mercado, e indicará si se autoriza su puesta en el mercado por cumplimiento de los requisitos esenciales establecidos en el momento de la emisión del dictamen o, por el contrario, si no se autoriza la puesta en el mercado por considerar que con la documentación presentada no se puede deducir que el aparato es conforme con los requisitos esenciales que le son aplicables.

6. Una vez recibido el dictamen por el solicitante, y en el caso de ser positivo, el aparato podrá ser puesto en el mercado europeo, tras haber cumplimentado lo dispuesto en el artículo 21. En el caso de dirigirse a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información para la aplicación de este procedimiento, se puede realizar la solicitud indicada en este capítulo y la notificación señalada en el artículo 21, de modo simultáneo.

7. Si en el plazo de cuatro semanas, contadas a partir de la recepción del expediente por el organismo notificado, no se hubiese obtenido respuesta en ningún sentido, el fabricante o su mandatario establecido en la Unión Europea, o el responsable de la puesta en el mercado, podrán poner en el mercado el aparato, marcado como se ha indicado anteriormente y en las condiciones previstas en este reglamento. En el caso de haber seleccionado la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información como organismo notificado, el plazo de los 28 días naturales quedará interrumpido si la documentación presentada es incompleta, mientras sea subsanada por el solicitante del dictamen técnico, de conformidad con el artículo 42.5.a) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.»

Cinco. El segundo párrafo del artículo 32 queda redactado de la siguiente manera:

«En el caso de elegir a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, presentará la solicitud ante dicha Secretaría de Estado. A tal efecto, podrá utilizarse el modelo que se incluye en el anexo III.2.»

Seis. El primer párrafo del apartado 2 del artículo 33 queda redactado de la siguiente manera:

«2. El organismo notificado hará evaluar, en particular, si el sistema de control de calidad asegura la conformidad de los aparatos con lo dispuesto en este reglamento, teniendo en cuenta la documentación presentada, incluidos, en su caso, los resultados de los ensayos facilitados por el fabricante.»

Siete. Los apartados 3 y 4 del artículo 33 quedan redactados de la siguiente manera:

«3. Cuando el organismo notificado sea la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, ésta estudiará la documentación indicada en el apartado 1 de este artículo y el resultado de la evaluación realizada según los criterios expuestos en el apartado 2, y emitirá la correspondiente autorización en un plazo no superior a dos meses. En el supuesto de que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información hubiera establecido requisitos adicionales, la autorización se concederá

en función de la evaluación de la entidad acreditada y del cumplimiento de los citados requisitos.

4. El fabricante se comprometerá a cumplir las obligaciones derivadas del sistema de calidad implementado, tal y como haya sido aprobado, y a mantenerlo de forma que conserve su adecuación y eficacia.

El fabricante o su mandatario informará al organismo notificado y a la entidad acreditada que le haya evaluado de cualquier adecuación que pretenda introducir en el sistema de calidad.

El organismo notificado hará evaluar las modificaciones propuestas y decidirá si el sistema de calidad modificado sigue cumpliendo los requisitos indicados anteriormente o, en caso necesario, efectuar una nueva evaluación, y comunicará su decisión al fabricante. La notificación contendrá las conclusiones del control y la decisión motivada de la evaluación.»

Ocho. La rúbrica y el apartado 1 del artículo 34 quedan redactados de la siguiente manera:

«Artículo 34. *Vigilancia CE del sistema de calidad.*

1. La finalidad de la vigilancia es cerciorarse de que el fabricante cumple correctamente con las obligaciones derivadas del sistema de calidad aprobado, que lo mantiene y lo aplica.

Para ello, el organismo notificado efectuará o hará efectuar, en las instalaciones del fabricante, las inspecciones y auditorías oportunas, y entregará al fabricante un informe con los resultados obtenidos.»

Nueve. El apartado 2 del artículo 41 queda redactado de la siguiente manera:

«2. En caso de disconformidad, se propondrá la incoación del correspondiente expediente sancionador, sin perjuicio de la aplicación de la medida cautelar prevista en el artículo 41 bis.»

Diez. Queda suprimido el apartado 5 del artículo 41.

Once. Se añade un artículo 41 bis, con la siguiente redacción:

«Artículo 41 bis. *Procedimiento de retirada del mercado de equipos y aparatos.*

La puesta en el mercado de equipos y aparatos de telecomunicación que no reúnan los requisitos que les son aplicables para su puesta en el mercado, de conformidad con lo establecido en este reglamento, que supongan un riesgo para la seguridad o salud de las personas o hayan causado o se considere justificadamente que puedan causar interferencias perjudiciales, o daños o perjuicios graves a la red, así como aquellos equipos y aparatos de telecomunicación para los cuales la Comisión Europea haya notificado una cláusula de salvaguardia, de acuerdo con lo establecido en el artículo 42, podrá dar lugar a la adopción por los Servicios de la Inspección de Telecomunicaciones de la medida cautelar consistente en la retirada del mercado de los correspondientes equipos y aparatos.

Dicha medida se mantendrá hasta la incoación del correspondiente expediente sancionador por los Servicios de la Inspección de Telecomunicaciones o hasta tanto se proceda, en su caso, a la verificación de la conformidad con los requisitos establecidos en este real decreto, sin perjuicio del dictamen de la Comisión Europea sobre las medidas de salvaguarda sobre aparatos de telecomunicaciones adoptadas por otros Estados miembros de la Unión Europea.

El procedimiento de retirada del mercado de los equipos y aparatos podrá realizarse por alguna de las siguientes modalidades:

a) Incautación y depósito en instalaciones o dependencias de la Administración competente.

b) Retirada de los equipos y aparatos por cuenta del fabricante o, en su defecto, por el responsable de su comercialización o puesta en el mercado.

El procedimiento de retirada del mercado de equipos y aparatos se sujetará a lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las

Administraciones Públicas y del Procedimiento Administrativo Común, y se podrá acordar por razones de interés público la aplicación del procedimiento de tramitación de urgencia.

De la medida cautelar adoptada se dará conocimiento a la Comisión Europea, a las asociaciones de fabricantes afectados, así como al Instituto Nacional del Consumo y al Consejo de Consumidores y Usuarios.»

Doce. El artículo 46 queda redactado de la siguiente manera:

«Artículo 46. *Organismo español notificado.*

En España se designa a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información como organismo notificado para la aplicación de las disposiciones de los capítulos III, IV y V del título III de este reglamento. El procedimiento de designación de otros organismos notificados en España se regulará mediante orden ministerial, en la que se determinará:

a) El alcance de la designación.
b) Los requisitos para obtener la designación.
c) Las causas de extinción de la designación.
d) Los derechos y obligaciones de las entidades designadas.»

Trece. Se añade una nueva disposición adicional al Real Decreto 1890/2000, de 20 de noviembre, por el que se aprueba el Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones, con la siguiente redacción:

«Disposición adicional segunda. *Notificación al Instituto Nacional del Consumo.*

Sin perjuicio del cumplimiento de lo dispuesto en el Reglamento que aprueba este Real Decreto, en aquellos casos en que los equipos y aparatos de telecomunicaciones supongan un riesgo grave para la salud y seguridad de los consumidores, por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, se remitirá la notificación correspondiente al Instituto Nacional del Consumo, según establece el Real Decreto 1801/2003, de 26 de diciembre, sobre seguridad general de los productos, salvo que se considere que el riesgo grave tiene efectos limitados al territorio español y no se prevea que pueda ser de interés su conocimiento en el ámbito de la Comunidad Europea.»

Disposición final cuarta. *Modificación del Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado por el Real Decreto 1066/2001, de 28 de septiembre.*

El Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado por el Real Decreto 1066/2001, de 28 de septiembre, se modifica en los siguientes términos:

Uno. El párrafo primero del apartado 1 del artículo 8 queda redactado de la siguiente manera:

«1. Los operadores que establezcan las redes o presten los servicios que se relacionan a continuación deberán presentar un estudio detallado, realizado por un técnico competente, que indique los niveles de exposición radioeléctrica en áreas cercanas a sus instalaciones radioeléctricas fijas en las que puedan permanecer habitualmente personas. Dichas redes o servicios son los siguientes:

a) Redes de difusión de los servicios de radiodifusión sonora y televisión.
b) Servicios de telefonía móvil automática analógica.
c) Servicio de telefonía móvil automática GSM.
d) Servicio de comunicaciones móviles personales DCS-1800.
e) Servicio de comunicaciones móviles de tercera generación.
f) Servicio de radiobúsqueda.

g) Servicio de comunicaciones móviles en grupo cerrado de usuarios.

h) Redes del servicio fijo por satélite, del servicio móvil por satélite y del servicio de radiodifusión por satélite.

i) Servicio de acceso vía radio LMDS.»

Dos. El párrafo segundo del apartado 3 del artículo 9 queda redactado de la siguiente manera:

«Asimismo, los operadores a los que se refiere el apartado 1 del artículo 8 deberán remitir al Ministerio de Industria, Turismo y Comercio, en el primer trimestre de cada año natural, una certificación emitida por un técnico competente de que se han respetado los límites de exposición establecidos en el anexo II durante el año anterior. Este ministerio podrá ampliar esta obligación a titulares de otras instalaciones radioeléctricas.»

Disposición final quinta. *Facultades de desarrollo.*

Se autoriza al Ministro de Industria, Turismo y Comercio a dictar las disposiciones necesarias para el desarrollo y aplicación de este real decreto.

Disposición final sexta. *Título competencial.*

Este real decreto se dicta al amparo de la competencia exclusiva sobre telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución.

Disposición final séptima. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO SOBRE LAS CONDICIONES PARA LA PRESTACIÓN DE SERVICIOS DE COMUNICACIONES ELECTRÓNICAS, EL SERVICIO UNIVERSAL Y LA PROTECCIÓN DE LOS USUARIOS

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto del reglamento.*

El objeto de este reglamento es la regulación de las condiciones para la prestación de servicios o la explotación de redes de comunicaciones electrónicas, en desarrollo del capítulo I del título II de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y de las obligaciones de servicio público y los derechos y obligaciones de carácter público aplicables en desarrollo del título III de dicha ley.

Artículo 2. *Sujetos obligados.*

Los derechos y obligaciones regulados en este reglamento serán aplicables a los operadores y, sin perjuicio de la aplicación del régimen sancionador del título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, a los que, sin haber efectuado la notificación a que se refiere el artículo 6 de dicha ley, exploten redes públicas de comunicaciones electrónicas o presten servicios de comunicaciones electrónicas disponibles al público.

Lo dispuesto en el capítulo I del título V de este reglamento será también de aplicación a quienes, sin estar comprendidos en el párrafo anterior, realicen actividades reguladas en la normativa sobre telecomunicaciones.

Artículo 3. *Régimen jurídico.*

El régimen jurídico general aplicable en la explotación de las redes y prestación de los servicios de comunicaciones electrónicas será el regulado en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en este reglamento y, en los términos previstos en el artículo 20 de la ley anteriormente citada, el régimen establecido para la concesión de servicio público del texto refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio.

TÍTULO II

Explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia

CAPÍTULO I

Régimen general de explotación de redes y de prestación de servicios de comunicaciones electrónicas

Artículo 4. *Requisitos generales.*

1. La explotación de las redes y la prestación de servicios de comunicaciones electrónicas se realizará en régimen de libre competencia, sin más limitaciones que las establecidas en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en este reglamento y en el resto de disposiciones que la desarrollen.

Conforme al artículo 8.4 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en la explotación de redes o servicios de comunicaciones electrónicas por las Administraciones públicas con contraprestación económica serán de aplicación las condiciones impuestas, en su caso, por la Comisión del Mercado de las Telecomunicaciones para garantizar la libre competencia.

La prestación transitoria por las entidades locales a sus ciudadanos de servicios de comunicaciones electrónicas de interés general sin contraprestación económica precisará su comunicación previa a la Comisión del Mercado de las Telecomunicaciones. Cuando ésta detecte que dicha prestación afecta al mercado, en función de la importancia de los servicios prestados, de la existencia en ese ámbito territorial de condiciones de mercado que permitan el acceso a dichos servicios o de la distorsión de la libre competencia, podrá imponer condiciones específicas a dichas entidades en la prestación de los servicios conforme al párrafo anterior.

2. Podrán explotar redes y prestar servicios de comunicaciones electrónicas a terceros las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o con otra nacionalidad cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

3. En todo caso, las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas a terceros deberán designar una persona responsable domiciliada en España a los efectos de notificaciones, sin perjuicio de lo que puedan prever los acuerdos internacionales. Se entenderá que el domicilio del representante coincide con el domicilio a los efectos de notificaciones de la persona representada.

4. La adquisición de los derechos de uso del dominio público radioeléctrico, de ocupación del dominio público o de la propiedad privada y de los recursos de numeración, direccionamiento o denominación necesarios para la explotación de redes o para la prestación de servicios de comunicaciones electrónicas deberá realizarse conforme a lo dispuesto en su normativa específica.

Artículo 5. *Notificación a la Comisión del Mercado de las Telecomunicaciones.*

1. Los interesados en la explotación de una determinada red o en la prestación de un determinado servicio de comunicaciones electrónicas deberán, con anterioridad al inicio de

la actividad, notificarlo fehacientemente a la Comisión del Mercado de las Telecomunicaciones, incluyendo la información que se señala en el apartado 5. Una vez realizada la notificación, el interesado adquirirá condición de operador y podrá comenzar la prestación del servicio o la explotación de la red.

2. Los operadores deberán notificar a la Comisión del Mercado de las Telecomunicaciones cada tres años, contados desde la notificación inicial, su intención de continuar con la prestación o explotación de la red o servicio. La condición de operador se mantendrá en tanto no se extinga conforme a lo establecido en el artículo 6.

3. Si la notificación no reúne los requisitos que se señalan en este artículo y no hubieran sido oportunamente subsanados en su caso los defectos formales, la Comisión del Mercado de las Telecomunicaciones, en un plazo no superior a 15 días, dictará resolución motivada, y la notificación se tendrá por no realizada. Contra dicha resolución podrá interponerse recurso contencioso-administrativo, de acuerdo con la ley reguladora de dicha jurisdicción.

4. No estarán sujetos a la obligación de la notificación:

a) La explotación de redes y la prestación de servicios de comunicaciones electrónicas en régimen de autoprestación.

b) Los servicios de comunicaciones electrónicas y las instalaciones de seguridad o intercomunicación que, sin conexión a redes exteriores y sin utilizar el dominio público radioeléctrico, presten servicio a un inmueble, a una comunidad de propietarios o dentro de una misma propiedad privada.

c) Los servicios de comunicaciones electrónicas establecidos entre predios de un mismo titular.

5. En la notificación prevista en el apartado 1 el interesado deberá incluir la siguiente información, junto con la documentación que acredite su autenticidad:

a) Cuando se trate de persona física:

1.º Nombre y apellidos y, en su caso, los de la persona que lo represente.

2.º Número del documento nacional de identidad o, si fuera extranjera, la nacionalidad y el número de pasaporte.

3.º Domicilio en España a los efectos de notificaciones.

4.º Documentación que acredite la capacidad y representación del representante, en su caso.

b) Cuando se trate de persona jurídica:

1.º Razón social.

2.º Número de identificación fiscal y datos registrales.

3.º Domicilio en España a los efectos de notificaciones.

4.º Nombre y apellidos de la persona responsable a los efectos de notificaciones.

5.º Documentación que acredite la capacidad y representación del representante.

Para personas jurídicas extranjeras nacionales de Estados miembros de la Unión Europea y de Estados signatarios del Acuerdo sobre el Espacio Económico Europeo, la documentación que acredite su capacidad de obrar consistirá en una certificación que acredite la inscripción en los registros que, de acuerdo con la legislación en cada Estado, sea preceptiva. Para el resto de personas jurídicas extranjeras será necesaria la presentación de una certificación expedida por la respectiva representación diplomática española en la que se haga constar que figuran inscritas en el Registro local profesional, comercial o análogo o, en su defecto, que actúan legalmente y con habitualidad en el ámbito de las actividades correspondientes.

c) En caso de ser una persona nacional de un Estado que no sea miembro de la Unión Europea, indicación del convenio internacional que le habilita para explotar redes o prestar servicios de comunicaciones electrónicas en España o, en su defecto, indicación del acuerdo del Consejo de Ministros que le autorice de forma excepcional.

d) Descripción de la red o servicio que el interesado tiene intención de explotar o prestar, que deberá incluir:

1.º Breve descripción de la ingeniería y diseño de red, en su caso.

2.º Tipo de tecnología o tecnologías empleadas.

3.º Descripción de las medidas de seguridad y confidencialidad que se prevén implantar en la red, en su caso.

4.º Descripción funcional de los servicios.
5.º Oferta de servicios y su descripción comercial.

e) La fecha prevista para el inicio de la actividad.
f) Sumisión a tribunales españoles y, si así lo desea el interesado, al arbitraje de la Comisión del Mercado de las Telecomunicaciones, en los términos establecidos en su reglamento y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para resolver las controversias que surjan en el ejercicio de su actividad.
g) Declaración responsable de cumplimiento de los requisitos exigibles.

Artículo 6. *Extinción de la habilitación.*

1. La habilitación para la explotación de redes o la prestación de servicios de comunicaciones electrónicas se extinguirá por las siguientes causas:
a) El cese en la actividad del operador habilitado, que deberá notificarse a la Comisión del Mercado de las Telecomunicaciones.
b) La extinción de la personalidad del operador.
c) Por sanción administrativa firme, de acuerdo con lo establecido en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
d) Por la falta de notificación a la Comisión del Mercado de las Telecomunicaciones de la intención del operador de continuar con la prestación o explotación de la red o servicio, que, conforme al artículo 5.2, debe efectuarse cada tres años. Para ello, se tramitará previamente un procedimiento contradictorio conforme al apartado siguiente, en el que se aprecie si se ha producido el cese en la actividad del operador.

2. La extinción de la condición de operador se establecerá por resolución de la Comisión del Mercado de las Telecomunicaciones, tras la tramitación del oportuno procedimiento. Dicho procedimiento será iniciado de oficio, en los siguientes términos:
a) En el supuesto del párrafo a) del apartado 1, tras la recepción de la notificación por el interesado.
b) En el supuesto del párrafo b), tras haber recibido noticia de la extinción de la personalidad.
c) En el supuesto del párrafo c), tras la recepción de la comunicación de la sanción impuesta por el Ministerio de Industria, Turismo y Comercio o, en su caso, tras la imposición de la sanción por la Comisión del Mercado de las Telecomunicaciones o por la Agencia Española de Protección de Datos.
d) En el supuesto del párrafo d), una vez haya transcurrido un mes desde la finalización del correspondiente plazo de tres años.

Las resoluciones por las que se declare la extinción de la condición de operador serán comunicadas al Ministerio de Industria, Turismo y Comercio.

CAPÍTULO II

Registro de operadores

Artículo 7. *Objeto del Registro de operadores.*

1. El Registro de operadores de redes y servicios de comunicaciones electrónicas tiene carácter administrativo, es de ámbito estatal, depende de la Comisión del Mercado de las Telecomunicaciones y su llevanza corresponderá, en los términos establecidos por este reglamento, al órgano que determinen las normas reguladoras de dicha Comisión.
2. El Registro de operadores (...) tiene por objeto la inscripción de las personas físicas o jurídicas que hayan realizado la notificación prevista en el artículo 5, de la red o servicio de comunicaciones electrónicas que pretenda explotar o prestar, de las condiciones aplicables al ejercicio de su actividad y de sus modificaciones.
3. La inscripción en el Registro de operadores tendrá carácter declarativo.

Artículo 8. *Acceso al registro y expedición de certificaciones.*

1. El Registro de operadores será público. Los asientos registrales contenidos en él serán de libre acceso para su consulta por cualquier persona que lo solicite.

Podrá también accederse a la consulta directa de los archivos y libros registrales. A estos efectos, el encargado del registro facilitará a los interesados la consulta de los asientos por medios informáticos instalados en la oficina del registro y, en su caso, a través de la página web de la Comisión del Mercado de las Telecomunicaciones.

2. Cualquier persona física o jurídica podrá solicitar certificaciones de operadores y demás actos inscritos. Las certificaciones registrales serán el único medio de acreditar fehacientemente el contenido de los asientos registrales. La expedición de certificaciones a instancia de parte dará lugar a la percepción de las tasas correspondiente con arreglo a lo previsto en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y en sus normas de desarrollo.

Artículo 9. *Estructura del registro.*

1. En el registro se llevarán libros de registro con la diligencia de apertura firmada por el Presidente de la Comisión del Mercado de las Telecomunicaciones y con expresión de los folios que contienen, que estarán numerados, sellados y rubricados. Se abrirá, en principio, un folio para cada operador.

2. A cada operador se le asignará en el libro correspondiente un número de inscripción que será el del folio en el que se inscriba. Dicho folio irá seguido de cuantos otros sean necesarios, ordenados, a su vez, con indicación del número que haya correspondido al folio inicial, seguido de otro que reflejará el número correlativo de folios que se precisen para la inscripción de las modificaciones que procedan.

3. Se podrán utilizar los libros auxiliares, archivos, cuadernos o legajos que el encargado del registro considere oportunos para su buen funcionamiento.

4. Todo lo previsto en los apartados anteriores podrá ser realizado por medios informáticos, siempre que éstos cuenten con el correspondiente soporte documental.

Artículo 10. *Inscripción en el registro.*

La primera inscripción será realizada de oficio por la Comisión del Mercado de las Telecomunicaciones en el plazo de 15 días contados desde la recepción de la notificación a que se refiere el artículo 5, siempre que cumpla todos los requisitos establecidos en dicho artículo. En dicha inscripción se consignarán los siguientes datos:

a) Respecto del operador:

1.º Nombre y apellidos o, en su caso, denominación o razón social, su nacionalidad y domicilio.

2.º Los datos relativos a la inscripción en el Registro Mercantil, en su caso.

3.º Su número o código de identificación fiscal, según proceda.

4.º El domicilio de la persona inscrita y el señalado a los efectos de notificaciones conforme a lo previsto en el artículo 4.3.

5.º El nombre y demás datos personales de su representante, en su caso.

6.º Nombre y apellidos de la persona responsable a los efectos de notificaciones.

b) En relación con la red o servicio de comunicaciones electrónicas que se pretenda explotar o prestar, se hará constar la fecha prevista de inicio del servicio y cuanta información haya tenido que ser aportada por el interesado, siempre que no tenga carácter confidencial.

Artículo 11. *Declaración normalizada de haberse producido la notificación e inscripción.*

Sin perjuicio de que las resoluciones de inscripción en el registro surtan los efectos de declaración normalizada de que el operador ha presentado la notificación, el operador podrá, en cualquier momento posterior, solicitar a la Comisión del Mercado de las Telecomunicaciones que emita una declaración normalizada que confirme que este ha presentado la notificación a la que se refiere el artículo 6 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y que ha resultado inscrito en el Registro de

operadores. La declaración detallará las circunstancias en que el operador tiene derecho a ocupar el dominio público o privado para la instalación de redes de comunicaciones electrónicas, negociar la interconexión y obtener el acceso o la interconexión.

Las declaraciones normalizadas serán emitidas por el Secretario de la Comisión del Mercado de las Telecomunicaciones, de acuerdo con el modelo aprobado por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, en el plazo de una semana desde que la solicitud haya tenido entrada en el registro de la Comisión.

Artículo 12. *Modificación de los datos inscritos.*

1. Una vez practicada la primera inscripción de un operador, se consignarán en el Registro cuantas modificaciones se produzcan respecto de los datos inscritos, tanto en relación con el titular como con la red o servicio de comunicaciones electrónicas que se pretenda explotar o prestar.

2. A los efectos de lo dispuesto en el apartado anterior, el operador estará obligado a comunicar a la Comisión del Mercado de las Telecomunicaciones las modificaciones que se produzcan respecto de los datos inscritos y a aportar la documentación que lo acredite fehacientemente. La comunicación deberá realizarse en el plazo máximo de un mes desde el día en que se produzca la modificación.

Cuando la modificación tenga su origen en un acto emanado del Ministerio de Industria, Turismo y Comercio o de la Comisión del Mercado de las Telecomunicaciones, la inscripción se realizará de oficio por esta última. A estos efectos, el Ministerio de Industria, Turismo y Comercio remitirá a la Comisión del Mercado de las Telecomunicaciones la correspondiente documentación.

3. En el caso de que la inscripción o sus modificaciones no pudieran practicarse por insuficiencia de los documentos aportados por el interesado, se le requerirá para que los complete en el plazo de 10 días.

4. Transcurrido el plazo para comunicar las modificaciones al que se refiere el apartado 2 o el de subsanación establecido en el apartado 3 sin que tal comunicación o subsanación se hayan producido, podrá iniciarse un expediente sancionador conforme a lo dispuesto en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 13. *Otros datos incluidos en el registro.*

1. Se practicará nota de oficio al margen de la inscripción correspondiente a los operadores que recoja la imposición de cualquier sanción firme impuesta de conformidad con el título VIII de la Ley 32/2003, de 3 de noviembre, y, en particular, se hará constar la inhabilitación del operador y la clausura provisional de instalaciones.

A los efectos de lo establecido en este apartado, el Ministerio de Industria, Turismo y Comercio y la Agencia Española de Protección de Datos comunicarán a la Comisión del Mercado de las Telecomunicaciones las resoluciones firmes y actos que, en el marco de sus respectivas competencias, impongan las sanciones y las medidas cautelares a que se refiere el párrafo anterior.

2. Asimismo, se hará constar, mediante nota practicada de oficio, si el operador se somete al arbitraje de la Comisión del Mercado de las Telecomunicaciones, en los términos establecidos en su reglamento y en la Ley 32/2003, de 3 de noviembre, para resolver las controversias que surjan en el ejercicio de su actividad.

3. Igualmente, podrán inscribirse como anotaciones preventivas las situaciones extrarregistrales que puedan afectar a los hechos inscritos.

4. Las notas y las anotaciones preventivas se cancelarán cuando conste que han dejado de concurrir los presupuestos que determinaron su práctica. En particular, las notas relativas a las sanciones se cancelarán una vez transcurridos los plazos establecidos en el artículo 57.2 de la Ley 32/2003, de 3 de noviembre.

Artículo 14. *Cancelación de la inscripción.*

1. La inscripción registral de un operador se cancelará cuando su habilitación se extinga por cualquiera de las causas establecidas en el artículo 6.2.

2. La cancelación de la inscripción se practicará de oficio por el encargado del registro al concluir el expediente previsto en el artículo 6.2.

3. El Ministerio de Industria, Turismo y Comercio y la Agencia Española de Protección de Datos comunicarán a la Comisión del Mercado de las Telecomunicaciones las resoluciones firmes en las que se acuerde la pérdida de la habilitación del operador, para que la citada entidad proceda a la cancelación de la correspondiente inscripción registral.

CAPÍTULO III

Condiciones para la explotación de redes y la prestación de servicios de comunicaciones electrónicas

Artículo 15. *Derechos de los operadores.*

Los operadores de redes y servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) Negociar y, en su caso, obtener la interconexión o el acceso a las redes y a los recursos asociados de otros operadores, conforme a la regulación establecida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y en la normativa sobre interconexión.

b) Obtener derechos de uso de la numeración, direccionamiento y denominación, de acuerdo con la regulación establecida en la Ley 32/2003, de 3 de noviembre, en el resto de normativa sobre numeración y en los planes nacionales de numeración, direccionamiento y denominación.

c) Obtener derechos de uso del dominio público radioeléctrico, conforme a la regulación establecida en la Ley 32/2003, de 3 de noviembre, y en sus disposiciones de desarrollo.

d) Obtener derechos de ocupación del dominio público y de la propiedad privada para la instalación de las redes de comunicaciones electrónicas, conforme a lo establecido en la Ley 32/2003, de 3 de noviembre, en este reglamento y el resto de normativa reguladora de la ocupación del dominio público y la propiedad privada.

e) Aquellos otros derechos reconocidos por la Ley 32/2003, de 3 de noviembre, por este reglamento y por el resto de disposiciones que la desarrollen.

Artículo 16. *Condiciones que deben cumplir los operadores.*

1. Los operadores estarán obligados al cumplimiento de las condiciones que se imponen en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en este reglamento y en el resto de la normativa que la desarrolle.

2. Las condiciones que se establecen en este capítulo se entienden sin perjuicio de otras condiciones que estén obligados a cumplir los operadores por alguno de los siguientes motivos:

a) Por razón del uso del dominio público radioeléctrico, de la numeración, direccionamiento y denominación o de la ocupación de la propiedad pública o privada para la instalación de redes.

b) Por ser designados para la prestación del servicio universal u otras obligaciones de servicio público.

c) Por la imposición, en su caso, de obligaciones específicas en el marco del análisis de mercado previsto en el artículo 10 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

d) Por la imposición de obligaciones en materia de interconexión y acceso previstas en el capítulo III del título II y en la disposición adicional séptima de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones

Artículo 17. *Condiciones generales.*

Las condiciones generales que deben cumplir todos los operadores, con independencia de la red o servicio que pretendan explotar o prestar, y sin perjuicio de otras que resulten exigibles conforme a los artículos siguientes de este capítulo, serán las siguientes:

a) Contribuir a la financiación del servicio universal, en los términos previstos en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarrollo.

b) Pagar las tasas previstas en el título VII de la Ley 32/2003, de 3 de noviembre, conforme a lo regulado en ella y en su normativa de desarrollo.

c) Garantizar la interoperabilidad de los servicios.

d) Garantizar a los usuarios finales la accesibilidad de los números, nombres o direcciones, de conformidad con lo recogido en los correspondientes planes nacionales.

e) Garantizar la protección de los datos personales y la intimidad de las personas, conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarrollo.

f) Garantizar a los consumidores y los usuarios finales los derechos que como tales les corresponden, de acuerdo con la Ley 32/2003, de 3 de noviembre, con este reglamento y con el resto de normativa que la desarrolle y con el resto de la normativa que resulte de aplicación.

g) Suministrar a las autoridades nacionales de reglamentación la información y documentación que precisen para el cumplimiento de sus fines, en los términos establecidos en el artículo 9 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y en el artículo 21 de este reglamento.

h) Ejecutar las órdenes de interceptación legal que emanen de la autoridad competente, conforme a la Ley de Enjuiciamiento Criminal y a la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, de acuerdo con lo establecido en el artículo 33 de la Ley 32/2003, de 3 de noviembre, y en el título V de este reglamento.

i) Cumplir, cuando así venga establecido en la normativa vigente, las resoluciones de las autoridades adoptadas por razones de interés público, de seguridad pública y de defensa nacional.

j) Asegurar el cumplimiento de las normas y especificaciones técnicas y los requisitos técnicos que, en cada caso, resulten aplicables, incluyendo los correspondientes en materia de equipos y aparatos de telecomunicaciones.

k) Cumplir las restricciones en cuanto a la transmisión de contenidos ilegales establecidas en la Ley 34/2002, de 11 de julio, sobre servicios de la sociedad de la información y comercio electrónico, y en relación con la transmisión de contenidos nocivos establecidas en la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, sobre la coordinación de disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva.

l) Cumplir el resto de requisitos y condiciones que se establecen en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarrollo.

Artículo 18. *Condiciones exigibles a los operadores que exploten redes públicas de comunicaciones electrónicas.*

Las condiciones que deben cumplir los operadores que exploten redes públicas de comunicaciones electrónicas serán las siguientes:

a) Garantizar la interconexión de las redes y el acceso a estas y a los recursos asociados, de conformidad con lo dispuesto en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarrollo.

b) Respetar las normas y resoluciones aprobadas por las autoridades competentes en materia de urbanismo, de medio ambiente y de ordenación del territorio, salud pública, seguridad pública, defensa nacional y tributación por ocupación del dominio público, conforme al artículo 28 de la Ley 32/2003, de 3 de noviembre, y a su normativa de desarrollo.

c) Respetar las normas y resoluciones aprobadas por las autoridades competentes en materia de acceso al dominio público y a la propiedad privada para la instalación de redes de comunicaciones electrónicas.

d) Cuando así sea preciso conforme a lo dispuesto en la Ley 32/2003, de 3 de noviembre, permitir la coubicación y el uso compartido de las instalaciones.

e) Respetar las limitaciones establecidas en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarrollo en relación con las emisiones radioeléctricas y la exposición del público a campos electromagnéticos.

f) Mantener la integridad de las redes públicas de comunicaciones electrónicas, así como evitar la producción de interferencias perjudiciales.

g) Procurar la seguridad de las redes públicas contra el acceso no autorizado y garantizar la confidencialidad de los mensajes transmitidos y el secreto de las comunicaciones.

h) Cumplir las obligaciones de extensión y cobertura establecidas en la disposición transitoria quinta de este reglamento.

i) Establecer condiciones de uso de sus redes o servicios para situaciones de catástrofes que garanticen las comunicaciones entre los servicios de emergencia y entre las autoridades, y para la difusión de informaciones a la población en general.

Artículo 19. *Condiciones exigibles a los operadores que exploten redes telefónicas públicas.*

Las condiciones que deben cumplir los operadores que exploten redes telefónicas públicas serán las siguientes:

a) Garantizar la integridad de la red desde una ubicación fija y, en caso de avería de la red debido a catástrofes o fuerza mayor, adoptar las medidas que establezca el Gobierno para garantizar la disponibilidad de la red telefónica pública y de los servicios telefónicos disponibles al público desde una ubicación fija.

b) Proporcionar a los usuarios a los que provea la conexión a la red telefónica el acceso a servicios de asistencia mediante operador y a los servicios de información sobre números de abonados previstos en el artículo 27.2.

c) Prestar las facilidades de marcación por tonos e identificación de la línea llamante, cuando sea técnicamente factible y económicamente viable.

d) Garantizar la conservación del número del abonado en los supuestos establecidos en la Ley 32/2003, de 3 de noviembre, y en su normativa de desarrollo.

e) Asegurar el encaminamiento gratuito de llamadas a los servicios de emergencia a través del número telefónico 112 y de otros números telefónicos que se determinen mediante real decreto.

Artículo 20. *Condiciones exigibles a los operadores que presten el servicio telefónico disponible al público.*

Las condiciones que deben cumplir los operadores que presten el servicio telefónico disponible al público serán las siguientes:

a) Cuando se preste el servicio desde una ubicación fija, se adoptarán las medidas necesarias para asegurar el acceso sin interrupciones a los servicios de emergencia.

b) Facilitar a la Comisión del Mercado de las Telecomunicaciones, para las finalidades previstas en el artículo 68, en soporte informático, como mínimo, los datos a los que se refiere el artículo 30.4 correspondientes a los abonados a los que ofrezcan la posibilidad de recibir llamadas a través de un número telefónico de abonado administrado por dichos operadores, incluyendo, de forma separada, los de aquellos que hubieran decidido no figurar en las guías. A estos efectos, estarán obligados a solicitar el consentimiento de los abonados conforme se indica en el artículo 67.

En caso de abonados de prepago, con los que no exista una relación contractual nominal, la aportación de datos se realizará previa solicitud y acreditación fehaciente por el abonado de su titularidad.

c) Asegurar la gratuidad de las llamadas a los servicios de emergencias. Esta obligación se exigirá respecto de las llamadas dirigidas al número telefónico 112 y a otros que se establezcan mediante real decreto, incluidas aquellas que se efectúen desde teléfonos públicos de pago, sin que sea necesario utilizar ninguna forma de pago en estos casos.

d) Poner a disposición de las autoridades receptoras de las llamadas a servicios de emergencias la información relativa a cada llamada sobre la ubicación de su procedencia, en la medida en que sea técnicamente viable, con respeto a la regulación establecida en el título VI y en las condiciones que se establezcan mediante orden ministerial.

e) Garantizar la conservación del número del abonado en los supuestos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y en su normativa de desarrollo.

f) Establecer condiciones de uso de sus redes o servicios para situaciones de catástrofes que garanticen las comunicaciones entre los servicios de emergencia y entre las autoridades, y para la difusión de informaciones a la población en general.

Artículo 21. *Obligaciones de suministro de información.*

1. Las autoridades nacionales de reglamentación establecidas en el artículo 46 de la Ley 32/2003, de 3 de noviembre, y los organismos con competencias inspectoras derivadas de dicha ley podrán, en el ámbito de su actuación, requerir a los operadores la información, incluso financiera, necesaria para el cumplimiento de alguna de las siguientes finalidades:

a) Comprobar el cumplimiento de las obligaciones que resulten de este capítulo, de los derechos de uso del dominio público radioeléctrico, de la numeración, direccionamiento y denominación o de la ocupación del dominio público o de la propiedad privada.

b) Satisfacer necesidades estadísticas o de análisis.

c) Evaluar la procedencia de las solicitudes de derechos de uso del dominio público radioeléctrico y de la numeración, direccionamiento y denominación.

d) Publicar síntesis comparativas sobre precios y calidad de servicio, en interés de los usuarios.

e) Elaborar análisis que permitan la definición de los mercados de referencia, la determinación de los operadores encargados de prestar el servicio universal y el establecimiento de condiciones específicas a los operadores con poder significativo de mercado en aquellos.

f) Cumplir los requerimientos que vengan impuestos en el ordenamiento jurídico.

g) Comprobar el cumplimiento del resto de obligaciones derivadas de la Ley 32/2003, de 3 de noviembre, y su normativa de desarrollo, en especial el cumplimiento de las obligaciones de servicio público y de carácter público.

Esta información, excepto aquella a que se refiere el párrafo c), no podrá exigirse antes del inicio de la actividad, y se suministrará en el plazo que se establezca en cada requerimiento, atendidas las circunstancias del caso. Las autoridades nacionales de reglamentación garantizarán la confidencialidad de la información suministrada que pueda afectar al secreto comercial o industrial.

2. Las solicitudes de información que se realicen de conformidad con el apartado anterior habrán de ser motivadas y proporcionadas al fin perseguido. En dichas solicitudes se indicará el plazo y grado de detalle con que deberá suministrarse la información requerida, así como los fines concretos para los que va a ser utilizada. El incumplimiento de la obligación de información por los titulares de redes o servicios de comunicaciones electrónicas podrá ser sancionado conforme a lo establecido en el título VIII de la Ley 32/2003, de 3 de noviembre.

3. La Comisión del Mercado de las Telecomunicaciones llevará a cabo la publicación, en la medida en que pueda contribuir al mantenimiento de un mercado abierto y competitivo, de la información que haya obtenido en el ejercicio de sus competencias, y garantizará la confidencialidad de la información y el derecho a la protección de los datos de carácter personal, conforme se indica en el apartado 1.

4. La información de que dispongan los operadores en relación con los servicios que presten al Ministerio de Defensa o instituciones militares no podrá ser facilitada en virtud de lo dispuesto en este artículo.

No obstante, lo dispuesto en el párrafo anterior, el Ministerio de Defensa aprobará una resolución en la que especificará de forma clara e inequívoca el tipo o categorías de información que puede ser suministrada. Esta resolución será comunicada a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y al resto de Autoridades de Reglamentación a que se refiere el artículo 46 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 22. *Modificación de las condiciones exigibles.*

1. Con arreglo a los principios de objetividad y proporcionalidad, el Gobierno, mediante real decreto, podrá modificar las condiciones impuestas en la prestación de servicios y el establecimiento y explotación de redes de comunicaciones electrónicas, y establecerá un plazo para que los operadores se adapten a dicha modificación.

2. En la tramitación de las modificaciones a que se refiere el apartado anterior se otorgará un trámite de audiencia, que no será inferior a cuatro semanas, a los interesados, al Consejo de Consumidores y Usuarios y, en su caso, a los sindicatos más representativos y a las asociaciones más representativas de los restantes usuarios. Asimismo, será preceptivo el informe de la Comisión del Mercado de las Telecomunicaciones.

TÍTULO III

Obligaciones de servicio público y de carácter público

CAPÍTULO I

Disposiciones generales

Artículo 23. *Categorías de obligaciones de servicio público o de carácter público.*

Tendrán la consideración de obligaciones de servicio público o de carácter público a los efectos de este reglamento:

a) El servicio universal, establecido en el artículo 22 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y regulado en el capítulo siguiente.

b) Las obligaciones de servicio público definidas en los apartados 1 y 2 del artículo 25 de la Ley 32/2003, de 3 de noviembre, que se regulan en el capítulo III de este título.

c) La obligación de encaminamiento y localización de llamadas dirigidas a servicios de emergencia. No obstante, la obligación de encaminamiento de dichas llamadas no dará lugar a contraprestación económica.

d) Las obligaciones de carácter público establecidas en este reglamento en relación con:

1.º El secreto de las comunicaciones y la obligación de interceptación legal, previstas en el capítulo II del título V de este reglamento.

2.º La regulación relativa a la protección de datos de carácter personal, desarrollada en el capítulo I del título V de este reglamento.

3.º Los aspectos específicos de los derechos de los consumidores y usuarios en relación con la prestación de los servicios de comunicaciones electrónicas desarrollados en el título VI de este reglamento.

4.º Las obligaciones de información previstas en el artículo 9 de la Ley 32/2003, de 3 de noviembre, y desarrolladas en el artículo 21 de este reglamento.

5.º Las obligaciones de calidad de servicio exigibles de conformidad con lo dispuesto en este reglamento, excepto las relativas a la prestación del servicio universal.

De conformidad con lo dispuesto en la Ley 32/2003, de 3 de noviembre, estas obligaciones de carácter público no darán derecho a contraprestación ni compensación económica de ningún tipo, sin perjuicio de lo dispuesto en el capítulo II del título V de este reglamento.

Artículo 24. *Sujetos obligados.*

Los operadores a que se refiere el artículo 2 estarán sujetos a las obligaciones de servicio público y a las demás obligaciones de carácter público que les sean de aplicación o, en su caso, impuestas, de conformidad con lo dispuesto en la Ley 32/2003, de 3 de noviembre, y en este reglamento.

En todo caso, el cumplimiento de las obligaciones de servicio público que sean exigibles a los operadores se efectuará con respeto a los principios establecidos en el artículo 20.3 de la Ley 32/2003, de 3 de noviembre.

Artículo 25. *Administración competente.*

Corresponde al Ministerio de Industria, Turismo y Comercio el control y el ejercicio de las facultades de la Administración reguladas en este título, sin perjuicio tanto de las competencias de la Comisión del Mercado de las Telecomunicaciones en relación con el servicio universal, de acuerdo con lo dispuesto en el capítulo II de este título, como de las de la Comisión Delegada del Gobierno para Asuntos Económicos y del Ministerio de Economía y Hacienda en materia de precios. A tales efectos, los operadores estarán obligados a cumplir las resoluciones que, en ejercicio de su función de control, dicten dicho ministerio, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y, cuando proceda, la Comisión del Mercado de las Telecomunicaciones. Dichas resoluciones serán motivadas, agotarán la vía administrativa y contra ellas podrá interponerse recurso contencioso-administrativo.

Artículo 26. *Principios aplicables en la imposición de obligaciones de servicio público.*

1. En la imposición de obligaciones de servicio público a los operadores se tomarán en consideración los objetivos y principios establecidos en el artículo 3 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. Cuando el Ministerio de Industria, Turismo y Comercio constate que cualquiera de los servicios a que se refiere este artículo se está prestando en competencia, en condiciones de precio, cobertura y calidad de servicio similares a aquellas en que los operadores designados deben prestarlas, podrá, previo informe de la Comisión del Mercado de las Telecomunicaciones y audiencia a los interesados, determinar el cese de su prestación como obligación de servicio público y, en consecuencia, de la financiación prevista para aquellas.

3. En particular, en la imposición de obligaciones de servicio público a los operadores serán de aplicación los siguientes criterios:

a) No imposición de cargas excesivas a los operadores que puedan afectar sustancialmente la posibilidad de su acceso al mercado.

b) Objetividad y transparencia en los métodos utilizados para determinar el operador obligado, las ayudas y financiación de la que disfrutará, y el momento y condiciones en que debe producirse.

c) No discriminación entre los distintos operadores, procurando mantener el equilibrio en el mercado de forma tal que ningún operador obtenga ventajas o desventajas en su actuación en el mercado, como consecuencia de las obligaciones impuestas.

d) Neutralidad económica y, en la medida de lo posible, tecnológica de las obligaciones impuestas y de las ayudas y financiación otorgadas.

e) Prioridad de las opciones que permitan un menor coste para el conjunto del sector o que supongan una menor necesidad de financiación.

CAPÍTULO II

Servicio universal

Sección 1.ª Delimitación del servicio universal

Artículo 27. *Concepto y delimitación de los servicios que se incluyen en el ámbito del servicio universal.*

1. Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible.

2. Bajo el concepto de servicio universal se deberá garantizar, en los términos y condiciones que se establecen en este capítulo, lo siguiente:

a) Que todos los usuarios finales puedan obtener una conexión a la red pública de comunicaciones electrónicas desde una ubicación fija con las características que se establecen en el artículo 28.1, siempre que sus solicitudes se consideren razonables en los términos establecidos en el artículo 29.

b) Que se satisfagan todas las solicitudes razonables de prestación de un servicio telefónico disponible al público a través de la conexión a que se refiere el párrafo anterior, que permitan efectuar y recibir llamadas nacionales e internacionales, con las características que se establecen en el artículo 28.2.

c) Que se ponga a disposición de los abonados al servicio telefónico disponible al público una guía general de números de abonados, de acuerdo con lo establecido en el artículo 30. Asimismo, que se ponga a disposición de todos los usuarios finales de dicho servicio un servicio de información general o consulta telefónica sobre números de abonados, en las condiciones establecidas en el artículo 31.

d) Que exista una oferta suficiente de teléfonos públicos de pago, u otros puntos de acceso público a la telefonía vocal, en todo el territorio nacional, de acuerdo con los términos que se establecen en el artículo 32.

e) Que los usuarios finales con discapacidad tengan acceso al servicio telefónico disponible al público desde una ubicación fija, a la guía general de números de abonados, al servicio de información general o consulta telefónica sobre números de abonados y al servicio de teléfonos públicos de pago, referidos en los apartados b), c) y d) anteriores, en condiciones equiparables a las que se ofrecen al resto de usuarios finales.

f) Que las personas con necesidades sociales especiales dispongan, de acuerdo con condiciones transparentes, públicas y no discriminatorias, de opciones o paquetes de tarifas que difieran de las aplicadas en condiciones normales de explotación comercial y que les permitan tener acceso al servicio telefónico disponible al público desde una ubicación fija o hacer uso de éste. Con el mismo objeto podrán aplicarse, cuando proceda, limitaciones de precios, tarifas comunes, equiparación geográfica u otros regímenes similares.

Artículo 28. *Conexión a la red pública y acceso al servicio telefónico disponible al público.*

1. La conexión a la red pública de comunicaciones electrónicas, desde una ubicación fija, referida en el apartado 2.a) del artículo anterior, provista a través de cualquier tecnología, deberá ofrecer a sus usuarios finales, de acuerdo con lo establecido en el artículo 29.1, la posibilidad de:

a) Conectar y utilizar los equipos terminales que sean conformes con la normativa aplicable y establecer comunicaciones telefónicas, y de fax de conformidad con las recomendaciones pertinentes de la serie T del UIT-T.

Asimismo, deberá disponer de los recursos técnicos adecuados para posibilitar la continuidad del servicio telefónico fijo disponible al público en situaciones de interrupción del suministro eléctrico por un periodo mínimo de cuatro horas. No obstante, en las conexiones a la red pública que se proporcionen a través de tecnologías que no permitan el suministro eléctrico desde las dependencias del operador, los recursos técnicos adecuados para garantizar la alimentación eléctrica de los equipos de terminación de red serán facilitados por el abonado.

b) Establecer comunicaciones de datos a velocidad suficiente para acceder de forma funcional a Internet. A estos efectos y en virtud de lo establecido en el artículo 52 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible, la conexión a la red deberá permitir comunicaciones de datos en banda ancha a una velocidad en sentido descendente de 1Mbit por segundo.

Dicho valor se refiere a la velocidad global de datos del enlace de usuario de acceso a la red, comprendiendo tanto la capacidad de transporte de datos neta que ofrece el enlace a cada usuario, como las taras de sincronización, control, operaciones, corrección de errores u otras funciones específicas del acceso. Para la tecnología ADSL esta velocidad global se corresponde con la de sincronización de los modems.

En relación con cada usuario el operador designado garantizará que la citada velocidad global de datos que debe proporcionar la conexión, promediada a lo largo de cualquier periodo de 24 horas, no sea inferior a un megabit por segundo.

Mediante Orden del Ministro de Industria, Turismo y Comercio se podrán establecer las definiciones y métodos de medida, de este parámetro relativo a la velocidad media ofrecida a cada usuario.

Asimismo, la conexión a la red deberá permitir que se pueda realizar sobre ella una prestación eficiente del servicio telefónico disponible al público, con las características mínimas referidas en el apartado 2 de este artículo, y de los servicios de datos, incluidos los de acceso a Internet, en condiciones equiparables a las ofrecidas, con carácter general, por el mercado. A tal efecto, el operador designado para el suministro de la conexión a la red deberá cumplir con alguno de los requisitos siguientes:

1.º Ofrecer a los prestadores de los citados servicios, existentes en el mercado, un tipo de acceso que permita realizar de forma eficiente su prestación. A tal efecto podrán establecerse requisitos mínimos a la conexión, considerándose en cualquier caso suficiente aquellos requisitos equiparables a los impuestos por la Comisión del Mercado de las Telecomunicaciones a los operadores con poder significativo en los mercados de acceso al servicio telefónico desde una ubicación fija y a servicios de datos.

2.º Asumir su prestación en las mencionadas condiciones, no siendo computable en tal caso el coste neto que ello le pudiera suponer a los efectos de la determinación del coste neto asociado al suministro de la conexión a la red.

2. El operador designado para la prestación del servicio telefónico disponible al público deberá satisfacer todas las solicitudes de acceso al servicio telefónico disponible al público sobre conexiones que posibiliten dicho acceso, de forma que permita al usuario recibir y efectuar llamadas telefónicas de ámbito nacional e internacional a través de números geográficos o no geográficos, de conformidad con lo establecido en el Plan nacional de numeración telefónica. Adicionalmente, deberá respetar en su prestación las condiciones de calidad y de asequibilidad que se establecen para el servicio telefónico disponible al público, respectivamente, en los artículos 34 y 35 de este reglamento.

Cuando se produzcan interrupciones de dicho servicio, por causas no atribuibles al abonado, el operador designado deberá compensarle de acuerdo con lo establecido en el artículo 15 de la carta de derechos del usuario de los servicios de comunicaciones electrónicas, aprobada por el Real Decreto 899/2009, de 22 de mayo.

Artículo 29. *Solicitudes de conexión a la red y plazo máximo de suministro.*

1. El operador designado para la prestación de este elemento de servicio universal deberá satisfacer las solicitudes razonables de conexión a la red pública de comunicaciones electrónicas desde una ubicación fija, con las prestaciones que le solicite el usuario dentro de las especificadas en el apartado 1 del artículo anterior. A estos efectos, el usuario podrá solicitar una conexión con las prestaciones establecidas en el apartado 1.a), en el 1.b), o ambas. Asimismo, el usuario podrá solicitar al operador designado las prestaciones del apartado 1.b) para una conexión existente que disponga de las contempladas en el apartado 1.a).

En cualquier caso, la contratación de la conexión no vinculará al usuario final para contratar otros servicios con el mismo operador. No obstante, la contratación de una conexión con unas determinadas capacidades podrá considerarse no razonable si no va acompañada de la contratación de alguno de los servicios ofertados sobre dichas capacidades por algún operador.

2. Sin perjuicio de lo establecido en el párrafo anterior, se considerarán en todo caso razonables las peticiones de conexión en las que se den alguna de las siguientes condiciones:

a) Que la conexión se solicite para cualquier inmueble situado en suelo urbano.

b) Que la conexión se solicite para una edificación, que aún no estando en suelo urbano, sea utilizada como vivienda habitual por el solicitante de conformidad con la normativa urbanística aplicable. Para su comprobación el operador designado podrá requerir al solicitante certificación del Ayuntamiento que acredite tales extremos.

3. Cuando dicho operador designado considere que una solicitud no es razonable y no se da ninguna de las dos condiciones anteriores, deberá someterla al Director General de Telecomunicaciones y Tecnologías de la Información, para la autorización de dicha consideración.

4. El operador designado deberá satisfacer cada solicitud razonable de conexión a la red pública de comunicaciones electrónicas, referidas en el punto 1 anterior, en un plazo máximo

de 60 días naturales, contados a partir de su recepción. Cuando dicha solicitud se realice conjuntamente con la de acceso al servicio telefónico disponible al público, se deberán satisfacer ambas en el mencionado plazo.

En caso de que para la realización del suministro sea necesario obtener permisos, derechos de ocupación o de paso específicos o por cualquier otra causa no imputable al operador, este podrá descontar los retrasos debidos a dichas causas, previa comunicación que contenga la acreditación documental necesaria de los retrasos remitida al solicitante por correo certificado con acuse de recibo en la que se informará al solicitante de la posibilidad de que dispone para presentar las reclamaciones a que se refiere el artículo 27 de la carta de derechos del usuario de los servicios de comunicaciones electrónicas, aprobada por el Real Decreto 899/2009, de 22 de mayo.

En el caso de no poder realizar el mencionado suministro en dicho plazo, una vez descontados los retrasos a que se refiere el párrafo anterior, sin mediar causas de fuerza mayor u otras imputables al solicitante, deberá compensar automáticamente a éste eximiéndole del pago de un número de cuotas mensuales relativas a la conexión equivalentes al número de meses o fracción en los que se haya superado dicho plazo.

5. La tramitación de las autorizaciones previstas en el apartado 3 se llevará a cabo por el procedimiento establecido en el Reglamento aprobado por el anexo I del Real Decreto 1773/1994, de 5 de agosto.

Artículo 30. *Guías telefónicas.*

1. Los abonados al servicio telefónico disponible al público tendrán derecho a disponer de una guía general impresa de números de abonados, que se actualice, como mínimo, una vez al año. Todos los abonados al servicio telefónico disponible al público tendrán derecho a figurar en la mencionada guía general, sin perjuicio, en todo caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad.

2. Cuando la disposición de la guía a la que se refiere este artículo no quede garantizada por el libre mercado, su elaboración, que se realizará teniendo en cuenta los principios de accesibilidad universal y diseño para todos, corresponderá a la empresa designada al efecto quien, además, habrá de entregarla gratuitamente a todos los abonados del servicio telefónico disponible al público. Cuando varios contratos de abono al servicio telefónico disponible al público estén domiciliados en la misma dirección, se entenderá cumplida dicha obligación entregando un ejemplar de la guía. Cuando, de acuerdo con lo especificado en el apartado 6 de este artículo, la guía se haya organizado en varios tomos, la empresa designada podrá limitar la entrega al tomo correspondiente a la demarcación territorial en que se incluya el domicilio del abonado, y pondrá a su disposición, gratuitamente, el resto de los tomos de la provincia.

3. La empresa designada podrá entregar a un abonado una guía telefónica en formato electrónico en lugar de la edición impresa, en las mismas condiciones que las establecidas para esta última en este artículo, siempre que incluya en dicha entrega formularios e indicaciones claras en forma impresa para la solicitud de la edición impresa. En caso de mediar solicitud por parte del abonado, dentro de los 30 días siguientes a la entrega de la guía electrónica, la empresa designada deberá entregar a dicho abonado la edición impresa en un plazo no superior a los 30 días, contados a partir de la recepción de la solicitud.

La empresa designada deberá ofrecer acceso a las guías telefónicas a través de Internet, en formato accesible para usuarios con discapacidad, en las condiciones y plazos de accesibilidad establecidos para las páginas de Internet de las administraciones públicas, en el reglamento aprobado por el Real Decreto1494/2007, de 12 de noviembre. Asimismo, de acuerdo con lo establecido en el artículo 35, facilitará a los usuarios ciegos o con grave discapacidad visual la franquicia al servicio de consulta telefónica sobre números de abonado que establezca la Comisión Delegada del Gobierno para Asuntos Económicos.

4. Sin perjuicio de lo dispuesto en el artículo 67, en relación con los datos relativos a cada abonado, deberá figurar, al menos, la siguiente información:

a) Nombre y apellidos, o razón social.
b) Número o números de abonado.
c) Dirección postal del domicilio, excepto piso, letra y escalera.

d) Terminal específico que deseen declarar, en su caso.

Cuando se trate del servicio telefónico fijo y el titular sea una persona física, podrá solicitar, al operador que le proporciona el servicio, que asociado a un mismo número figure el nombre de otra persona mayor de edad con la que conviva. La solicitud de alta de dicha inscripción se realizará de forma conjunta, mientras que para la baja bastará con la solicitud del interesado. Cuando se trate del servicio telefónico fijo y el titular sea una entidad u organización que tenga asignada una pluralidad de números, el operador del cual dependan esos números deberá asegurarse de que figuren, debidamente ordenadas, las inscripciones necesarias, para facilitar la localización de los números de los usuarios externamente más relevantes de dicha entidad u organización.

5. En las hojas iniciales de cada ejemplar de guía telefónica se facilitará, al menos, la siguiente información:

a) La dirección postal y números telefónicos de atención al usuario de los proveedores del servicio telefónico disponible al público de los que dependa alguno de los números que figuran en ese ejemplar.

b) Información a los abonados sobre su derecho a no figurar en una guía accesible al público o, en su caso, a que se omita parcialmente su dirección o algún otro dato, en los términos que haya estipulado su proveedor, a que sus datos que aparezcan en la guía no sean utilizados con fines de publicidad o prospección comercial y sobre el ejercicio de los derechos de acceso, oposición, rectificación y cancelación de sus datos, en los términos previstos por la legislación vigente en materia de protección de datos de carácter personal.

c) Instrucciones que indiquen cómo acceder y hacer uso de la guía telefónica y del servicio telefónico disponible al público.

d) Las direcciones postales y números telefónicos de los servicios públicos en materia de atención de urgencias sanitarias, de extinción de incendios y salvamento, de seguridad ciudadana y de protección civil.

e) Los números de los servicios de consulta sobre números de abonado.

f) Fecha completa de edición y actualización, así como nombre y dirección del editor.

g) Información relativa al departamento o servicio especializado de atención al cliente, de los prestadores del servicio universal al que se refiere el artículo 26 de la carta de derechos del usuario de los servicios de comunicaciones electrónicas, aprobada por el Real Decreto 899/2009, de 22 de mayo.

6. Los datos que figuren en las guías telefónicas estarán recogidos en un tipo de letra claro y de fácil lectura. La impresión se realizará preferentemente a dos caras, utilizando un papel con una textura que permita dicha impresión sin dificultar la lectura de la información. La encuadernación deberá soportar sin deterioro un uso normal durante la vigencia de la guía.

Los datos estarán relacionados por orden alfabético del primer apellido o razón social. Después del primer apellido se reflejará completo el segundo, seguido tras una coma, del nombre propio o de sus iniciales. Asociado a cada número figurará, además, la dirección del abonado, sin especificación de piso o letra, y, en su caso, un identificador del tipo de terminal (teléfono normal, fax, RDSI, videoconferencia, telefonía móvil, telefonía de texto para personas sordas, entre otros) que el abonado haya manifestado su deseo de que figure de forma tal que permita tener constancia del contenido de la solicitud y la identidad del solicitante.

Con carácter general y dentro del ámbito provincial de las guías telefónicas, su contenido se organizará por orden alfabético de los términos municipales y, en su caso, de entidades locales menores, salvo la capital de la provincia que aparecerá en primer lugar. Dentro de cada término o entidad local menor se organizará por la letra del primer apellido o razón social.

Cuando el número de abonados de una provincia sea elevado, la guía telefónica se podrá organizar territorialmente en varios tomos para facilitar su manejo. La división de la información provincial para su inclusión en cada tomo se realizará de modo que se facilite su uso, teniendo especialmente en cuenta para ello la demanda y utilización habitual de la información por los usuarios del servicio telefónico disponible al público.

La información relativa a los abonados de distintos servicios telefónicos o de diferentes operadores deberá tener un tratamiento tipográfico equivalente.

Sin perjuicio de lo establecido en el artículo 67, la guía general de números de abonados que se incluye en el ámbito del servicio universal deberá actualizarse, cómo mínimo, cada 12 meses. En cada actualización se incluirán todas las rectificaciones, altas y bajas que hayan sido comunicadas con anterioridad al cierre de la edición. El período comprendido entre la fecha de actualización de los datos y la fecha de edición de las guías telefónicas no podrá superar los tres meses.

7. En relación con los datos de carácter personal relativos a cada abonado incluidos en las guías, así como a sus derechos, será de aplicación lo establecido en el capítulo I del título V de este reglamento y la legislación vigente en materia de protección de datos de carácter personal.

Artículo 31. *Servicio de consulta telefónica sobre números de abonado.*

Los usuarios finales del servicio telefónico disponible al público tendrán derecho a disponer de un servicio de consulta telefónica sobre los números de abonado contenidos en las guías telefónicas a las que se refiere el artículo 30, actualizado y de ámbito nacional.

Este servicio se prestará a un precio asequible y con los objetivos de calidad que se fijen de acuerdo con el procedimiento establecido en el artículo 34.

En relación con los datos personales relativos a cada abonado, será de aplicación lo establecido en el capítulo I del título V y en la demás normativa vigente en cada momento sobre protección de los datos personales.

Artículo 32. *Teléfonos públicos de pago u otros puntos de acceso público a la telefonía vocal.*

1. En la prestación del servicio universal se deberá garantizar la existencia de una oferta suficiente de teléfonos públicos de pago u otros puntos de acceso público a la telefonía vocal. A estos efectos, se consideran teléfonos públicos de pago los situados en el dominio público de uso común. Mediante Orden del Ministerio de Industria, Turismo y Comercio se podrán especificar otros puntos de acceso público a la telefonía vocal y las condiciones de integración en la oferta suficiente de puntos de acceso público a la telefonía vocal.

El operador designado para la prestación de este elemento deberá garantizar la existencia de una oferta suficiente de teléfonos públicos de pago en la zona correspondiente a la designación, con las condiciones técnicas mínimas que se establecen en el apartado 3.

Se considerará oferta suficiente la existencia, con una distribución geográfica razonable, de, al menos, un teléfono público de pago y uno más por cada 3.000 habitantes en cada municipio de 1.000 o más habitantes y de un teléfono público de pago en cada uno de los municipios de menos de 1.000 habitantes en los que esté justificado sobre la base de la existencia de una distancia elevada a facilidades similares, la baja penetración del servicio telefónico fijo, la falta de accesibilidad del servicio telefónico móvil o la elevada tasa de población flotante.

El operador designado deberá satisfacer, en un plazo razonable, todas las solicitudes de instalación de nuevos teléfonos públicos de pago que le presenten los ayuntamientos hasta cumplir con los criterios de oferta suficiente.

Asimismo, el operador designado deberá mantener la oferta de ubicaciones y terminales de telefonía de pago con equipos de tecnología adecuada. No obstante, podrá realizar las modificaciones de dicha oferta, incluyendo cambios de ubicación y retirada de terminales cuando se sobrepase el criterio de oferta mínima, que sean necesarias para mantener la adecuación de la oferta a las necesidades de los usuarios. Dichas modificaciones se podrán realizar previa comunicación motivada al ayuntamiento correspondiente y siempre que este no haya manifestado su oposición igualmente motivada en el plazo de un mes a partir de dicha comunicación.

Cuando el operador designado considere que una solicitud de instalación de nuevos teléfonos públicos de pago o una oposición a la modificación de la oferta, presentada por algún ayuntamiento, no se corresponde con las obligaciones de servicio universal, podrá dirigirse a la Dirección General de Telecomunicaciones y Tecnologías de la Información, la cual resolverá siguiendo el mismo procedimiento que el indicado en el artículo 29.5.

2. Para la elección de las nuevas ubicaciones se tendrán en cuenta las zonas o lugares más transitados y de mayor demanda potencial, así como aquellas otras con escasa penetración del servicio telefónico fijo disponible al público.

3. Los teléfonos públicos de pago a los que se refiere este artículo deberán:

a) Ofrecer a los usuarios la posibilidad de realizar llamadas con destino a cualquier abonado del servicio telefónico disponible al público, respetando su carácter gratuito, en su caso.

b) Permitir efectuar gratuitamente llamadas de emergencia sin tener que utilizar ninguna forma de pago, utilizando el número único de llamadas de emergencia 112 y demás números de emergencia que estén definidos como gratuitos por la normativa vigente en cada momento.

c) Permitir su uso durante las 24 horas del día, contando con iluminación suficiente durante las horas nocturnas.

d) Disponer del aislamiento acústico necesario para proteger al usuario del ruido exterior y asegurar un nivel adecuado de privacidad de las comunicaciones.

e) Incorporar una pantalla electrónica que indique el número marcado, el crédito mínimo exigido y el crédito disponible, y sistemas ópticos y acústicos de aviso de finalización de crédito.

f) Disponer, en lugar visible, de información adecuada y actualizada sobre las condiciones básicas de uso del servicio y sobre sus precios, en la que se incluirá en todo caso indicación sobre el carácter gratuito de las llamadas de emergencias al servicio 112, así como, en su caso, los demás servicios de emergencias que estén definidos como gratuitos por la legislación vigente en cada momento y sobre el servicio de consulta telefónica sobre números de abonado al que se refiere el artículo 31.

g) Disponer de medidas de seguridad adecuadas contra el vandalismo y contra su utilización indebida.

h) Efectuar el cobro de la comunicación al final de esta y devolver el saldo sobrante sobre la base de las monedas previamente depositadas. En el caso de pago con tarjeta, el cobro se efectuará al finalizar la comunicación.

Además, las nuevas instalaciones de teléfonos públicos de pago deberán ofrecer las opciones de pago por monedas y por tarjeta. Cuando se instalen de forma agrupada, dichas opciones deberán ser ofrecidas por el conjunto de los teléfonos públicos de pago de la agrupación.

i) Permitir el acceso gratuito al servicio de consulta telefónica sobre números de abonado referido en el artículo 31.

4. El operador designado deberá mejorar progresivamente las condiciones de accesibilidad de los teléfonos públicos de pago a los que se refiere este artículo, teniendo en cuenta: la necesaria compatibilidad con el uso por personas con discapacidad, los estándares internacionales sobre accesibilidad aplicados en los países más avanzados, las normas de las distintas Administraciones públicas españolas y los trabajos de las organizaciones más representativas de personas con discapacidad, así como la distribución de la demanda y la climatología de las distintas zonas del territorio.

Para ello, el operador designado presentará, para su aprobación por el Ministerio de Industria, Turismo y Comercio, planes de adaptación de los teléfonos públicos de pago para facilitar su accesibilidad por los usuarios con discapacidad y, en particular, por los usuarios ciegos, sordos, en silla de ruedas o de talla baja. En relación con los usuarios ciegos, los planes deberán contemplar la accesibilidad, tanto de la información dinámica facilitada por el visor de terminal, como de la estática a la que se refiere el apartado 3.f) de este artículo. Dichos planes se deberán presentar con un año de antelación a la finalización del que estuviera vigente o cuando el Ministerio de Industria, Turismo y Comercio lo demande por considerar superado el vigente.

Artículo 33. *Otras medidas para facilitar la accesibilidad al servicio por las personas con discapacidad.*

1. De acuerdo con lo dispuesto en el artículo 27.2.e), los operadores designados para la prestación del servicio telefónico disponible al público referido en el artículo 27.2.b), o para la prestación de los servicios de directorio referidos en el artículo 27.2.c), o para la prestación

del servicio de teléfonos públicos de pago referido en el artículo 27.2.d) deberán garantizar que los usuarios finales con discapacidad tengan acceso a dichos servicios a un nivel equivalente al que disfrutan el resto de usuarios finales.

Dentro del colectivo de las personas con discapacidad, se considerarán incluidas las personas ciegas o con grave discapacidad visual, las personas sordas o con grave discapacidad auditiva, las personas con graves problemas en el habla y, en general, cualesquiera otras con discapacidades físicas que les impidan manifiestamente el acceso normal al servicio telefónico fijo o le exijan un uso más oneroso de este.

2. A los efectos de lo dispuesto en el apartado anterior, el operador designado para la prestación del servicio telefónico disponible al público referido en el artículo 27.2.b), garantizará la existencia de una oferta suficiente y tecnológicamente actualizada de terminales especiales, adaptados a los diferentes tipos de discapacidades, tales como teléfonos de texto, videoteléfonos o teléfonos con amplificación para personas sordas o con discapacidad auditiva, o soluciones para que las personas con discapacidad visual puedan acceder a los contenidos de las pantallas de los terminales, y realizará una difusión suficiente de aquélla.

Los abonados ciegos o con discapacidad visual, previa solicitud al operador designado, dispondrán de las facturas y la publicidad e información, suministrada a los demás abonados de telefonía fija sobre las condiciones de prestación de los servicios, en sistema Braille o en letras grandes o bien en un formato electrónico accesible, según sea su necesidad para el acceso apropiado a la información.

El operador designado aplicará a los usuarios con ceguera o con discapacidad visual grave, y a aquellos abonados en cuya unidad familiar exista alguna persona en tales circunstancias, una franquicia de 10 llamadas mensuales gratuitas al servicio de consulta telefónica sobre números de abonado.

Artículo 34. *Condiciones relativas a la calidad.*

El operador designado deberá cumplir en relación con el conjunto de sus usuarios finales, en todo el territorio y para todos los servicios abarcados por dicha designación, con los niveles mínimos de calidad de servicio que se establezcan por orden ministerial, y mantendrá una razonable uniformidad en las distintas zonas del territorio y en relación con los distintos tipos de usuarios.

Cuando de la aplicación de los niveles de calidad de servicio al conjunto de los usuarios, según lo previsto en el párrafo anterior, se deriven desviaciones significativas para determinadas zonas o tipos de usuarios que supongan para dichos grupos unos niveles peores a los fijados con carácter general, el Ministerio de Industria, Turismo y Comercio podrá establecer ámbitos de análisis más restringidos y fijar para dichos ámbitos niveles mínimos de calidad de servicio que limiten las mencionadas desviaciones con el objetivo de subsanar los efectos prácticos no deseados derivados del establecimiento de dichos niveles con carácter general.

Las definiciones y métodos de medida de los parámetros de calidad de servicio, los requerimientos relativos a la remisión periódica de los datos a la Administración, las condiciones orientadas a garantizar la fiabilidad y la posibilidad de comparación de los datos y las demás condiciones relativas a la medida y seguimiento de los niveles de calidad de servicio serán las establecidas mediante orden ministerial.

Los parámetros que se establezcan en dicha orden incluirán los que figuran en la norma del Instituto Europeo de Normas de Telecomunicación ETSI EG 202 057 y el desglose regional será, como mínimo, por comunidad autónoma.

Sección 2.ª Carácter asequible del precio del servicio universal

Artículo 35. *Concepto y objetivos.*

1. La Comisión Delegada del Gobierno para Asuntos Económicos, a propuesta de los Ministros de Industria, Turismo y Comercio y de Economía y Hacienda, y previo informe de la Comisión del Mercado de las Telecomunicaciones, garantizará el carácter asequible de los precios de los servicios incluidos dentro del servicio universal.

Serán objeto de especial consideración los colectivos de pensionistas y jubilados de renta familiar baja y el colectivo de las personas con discapacidad a las que se refiere el artículo 33.1.

Se entenderá que los precios de los servicios incluidos en el servicio universal son asequibles para los usuarios cuando se cumplan los siguientes objetivos:

a) Que los precios de los servicios incluidos en el servicio universal en zonas de alto coste, rurales, insulares y distantes sean comparables a los precios de dichos servicios en áreas urbanas, teniendo en cuenta, entre otros factores, sus costes y los colectivos con necesidades sociales especiales conforme a este reglamento.

b) Que se asegure la eliminación de barreras de precios que impidan a las personas con discapacidad el acceso y uso de los servicios incluidos en el servicio universal en condiciones equivalentes al resto de usuarios.

c) Que exista una oferta suficiente, a precio uniforme, de teléfonos de uso público en el dominio público de uso común, en todo el territorio abarcado por cada designación. Los precios de las llamadas realizadas desde estos terminales deberán ser comparables a los de las realizadas por los abonados en aplicación del apartado a) anterior, teniendo en cuenta los costes unitarios de su prestación a través de teléfonos públicos de pago.

d) Que se ofrezcan planes de precios en los que el importe de las cuotas de alta, el de los conceptos asimilados y el de las cuotas periódicas fijas de abono no limiten la posibilidad de ser usuario del servicio.

e) Que el servicio de consulta telefónica sobre números de abonado, referido el artículo 31, esté accesible a todos los usuarios del servicio telefónico disponible al público a precios que no supongan una limitación a las necesidades de utilización del mismo por los usuarios.

2. Para alcanzar los objetivos citados en el apartado anterior, el operador designado, según proceda, deberá ofrecer a sus abonados:

a) Programas de precios de acceso y uso de los servicios incluidos en el servicio universal que permitan el máximo control del gasto por parte del usuario y, en particular, los siguientes:

1.º Abono social. Este plan de precios estará destinado a jubilados y pensionistas cuya renta familiar no exceda del indicador que se determine, en cada momento, por la Comisión Delegada del Gobierno para Asuntos Económicos, y consistirá en la aplicación de una bonificación en el importe de la cuota de alta y en la cuota fija de carácter periódico de la conexión a la red.

2.º Usuarios ciegos o con grave discapacidad visual. Consistirá en la aplicación de una determinada franquicia en las llamadas al servicio de consulta telefónica sobre números de abonado, y en el establecimiento de las condiciones para la recepción gratuita de las facturas y de la publicidad e información suministrada a los demás abonados de telefonía fija sobre las condiciones de prestación de los servicios, en sistema Braille o en letras grandes o bien en un formato electrónico accesible, según sea su necesidad para el acceso apropiado a la información.

3.º Usuarios sordos o con discapacidad auditiva grave o personas con graves problemas en el habla. Este plan especial de precios se aplicará a las llamadas realizadas desde cualquier punto del territorio nacional que tengan como origen o destino un terminal de telefonía de texto y que se establezcan a través del centro de servicios de intermediación para teléfonos de texto.

b) Posibilidad de que el usuario elija la frecuencia de facturación que mejor se adapte a sus preferencias, dentro de las posibilidades ofertadas por el operador, las cuales incluirán, como mínimo, la frecuencia mensual.

c) Posibilidad de restringir y bloquear por parte de los usuarios, a través de un procedimiento sencillo y sin coste alguno, las llamadas internacionales y las que se hagan a servicios con tarificación adicional. Todo ello sin perjuicio de que se pueda seguir realizando el mismo tipo de llamadas a través de mecanismos de selección de operador cuando tengan contratado el servicio con algún otro proveedor sin la restricción o el bloqueo de los mencionados tipos de llamadas.

d) Publicidad e información sobre las condiciones de prestación de los servicios, especialmente con relación al principio de accesibilidad y de asequibilidad de estos.

e) Un nivel básico y gratuito de detalle en las facturas, para que los consumidores puedan comprobar y controlar los gastos generados por el uso de los servicios, así como efectuar un seguimiento adecuado de sus propios gastos y utilización, ejerciendo con ello un nivel razonable de control sobre sus facturas.

f) Medios para el abono previo, así como la posibilidad de efectuar el pago de la conexión de manera escalonada, cuando así se establezca por resolución del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

3. La Comisión del Mercado de las Telecomunicaciones elaborará un informe anual sobre la evolución y el nivel de la tarificación al público aplicable a los servicios pertenecientes a las obligaciones de servicio universal y que sean prestados por empresas designadas, en particular en relación con los niveles nacionales de precios al consumo y de rentas.

Sección 3.ª Operadores obligados a la prestación. Procedimiento de designación de operadores

Artículo 36. *Designación de operador para la prestación del servicio universal.*

1. Cuando la prestación de cualquiera de los elementos integrantes del servicio universal no quede garantizada por el libre mercado, el Ministerio de Industria, Turismo y Comercio designará uno o más operadores para que garanticen la prestación eficiente del servicio universal, de manera que quede cubierta la totalidad del territorio nacional. A estos efectos, podrán designarse operadores diferentes para la prestación de los diversos elementos del servicio universal y abarcar distintas zonas del territorio nacional.

La determinación de aquellas zonas geográficas y elementos integrantes del servicio universal en donde no queden garantizadas sus prestaciones por el libre mercado se realizará por el Ministerio de Industria, Turismo y Comercio, previo informe preceptivo de la Comisión del Mercado de las Telecomunicaciones en el que se constate la zona y el elemento cuya prestación no queda garantizada por el libre mercado.

El sistema de designación de operadores encargados de garantizar la prestación de los servicios, elementos y ofertas del servicio universal que se establece en los artículos siguientes de este reglamento se sujeta, en todo caso, a los principios de publicidad, concurrencia, igualdad, eficacia y no discriminación, así como a los restantes establecidos en el capítulo I de este título. Estos procedimientos de designación se podrán utilizar como medio para determinar el coste neto derivado de las obligaciones asignadas, a los efectos de lo dispuesto en las secciones siguientes de este capítulo.

2. Una vez finalizado el proceso de designación, el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, podrá dictar las instrucciones necesarias, en su caso, para proceder de forma ordenada al cese del cumplimiento de las obligaciones de servicio universal y su asunción por el nuevo operador u operadores que como consecuencia de dicho proceso hubiesen resultado designados.

3. Cuando un operador designado para la prestación del servicio universal se proponga entregar una parte o la totalidad de sus activos de red de acceso local a una persona jurídica independiente informará al Ministerio de Industria, Turismo y Comercio a fin de que éste, previo informe de la Comisión del Mercado de las Telecomunicaciones, pueda evaluar las repercusiones de la operación prevista en el suministro de acceso desde una ubicación fija y la prestación de servicios telefónicos, y en su caso, imponer, modificar o suprimir obligaciones específicas de conformidad con lo establecido en la Ley General de Telecomunicaciones y su normativa de desarrollo.

4. La designación de un operador para la prestación del servicio universal dará lugar, en el caso de que la prestación para la que ha sido designado implique un coste neto que suponga una carga injustificada, a la calificación de dicho operador como receptor de fondos del Fondo nacional de financiación del servicio universal o, en su defecto, del mecanismo de compensación entre operadores que se establece en este reglamento.

Artículo 37. *Prestación del servicio universal mediante licitación.*

1. El procedimiento para designar a un operador encargado de garantizar la prestación de un elemento del servicio universal en una determinada zona se iniciará, con una antelación de al menos seis meses a la finalización del período vigente, por el Ministerio de Industria, Turismo y Comercio con la puesta en marcha del procedimiento de licitación previsto en este artículo.

2. El titular del Ministerio de Industria, Turismo y Comercio efectuará, mediante orden ministerial, la convocatoria del correspondiente concurso y la publicación de las bases en las que se determinará el servicio o elemento que se debe prestar, el ámbito territorial, el período y las condiciones de prestación y financiación del servicio, de conformidad con lo establecido en este reglamento y en la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, previo informe de la Comisión del Mercado de las Telecomunicaciones y de la Comisión Delegada del Gobierno para Asuntos Económicos.

En los criterios de adjudicación que se incluyan en dichas bases al menos se deberán tener en cuenta los relativos a la eficiencia económica mediante el menor coste neto, a las mejores prestaciones para los usuarios y a las garantías de continuidad en la prestación del elemento de servicio universal del que se trate. En la determinación de las zonas de designación predominará el criterio de eficacia.

Asimismo, las bases contemplarán la determinación del coste neto para todo el periodo de la designación, en base a la oferta presentada por el licitante de acuerdo con la metodología para determinar el coste neto establecida previamente por la Comisión del Mercado de las Telecomunicaciones, o la determinación de un límite superior de coste neto libremente ofertado por el licitante, en función de la propuesta presentada que se considere más eficiente desde el punto de vista económico.

Los servicios o elementos integrantes del servicio universal susceptibles de ser objeto de licitación, en determinadas zonas, son:

a) El de conexión a red pública de comunicaciones electrónicas, referido en el artículo 28.1.

b) La prestación del servicio telefónico disponible al público, referido en el artículo 28.2.

c) La prestación de una oferta suficiente de teléfonos públicos de pago, referido en el artículo 32.

d) La elaboración de las guías telefónicas a las que se refiere el artículo 30.

e) La prestación del servicio de consulta telefónica sobre números de abonado al que se refiere el artículo 31.

3. Podrá presentarse al concurso cualquier persona física o jurídica legalmente establecida.

4. El Ministerio de Industria, Turismo y Comercio adjudicará el concurso al licitador que ofrezca las condiciones más ventajosas. En consecuencia, la empresa que resulte adjudicataria tendrá la consideración de operador designado para la prestación del servicio universal.

5. En el supuesto de que el concurso sea declarado desierto, la designación del operador encargado de prestar el servicio universal se realizará conforme al artículo siguiente.

Artículo 38. *Prestación del servicio universal por designación directa.*

Cuando un concurso de designación de operador en relación con un elemento y zona determinadas haya sido declarado desierto, mediante orden del Ministerio de Industria, Turismo y Comercio se podrá designar para dicho elemento y zona a cualquier operador que tenga poder significativo en mercados que incluyan ese elemento y zona, o se encuentre designado en esos momentos para su prestación. Cuando en una zona determinada no existieran operadores con dicho poder significativo de mercado, ni con designación en vigor, se podrá designar, previa consulta a las partes implicadas, a cualquiera de los operadores con mayor cuota de participación en dichos mercados.

En la orden a la que se refiere el párrafo anterior, previo informe de la Comisión del Mercado de las Telecomunicaciones y de la Comisión Delegada del Gobierno para Asuntos Económicos, se establecerá el servicio o elemento que se deba prestar y en qué ámbito

territorial, así como el período y las condiciones de prestación del servicio, todo ello de conformidad con lo establecido en este reglamento.

Sección 4.ª Coste neto de la prestación del servicio universal

Artículo 39. *Concepto de coste neto.*

1. El coste neto de las obligaciones del servicio universal se obtendrá hallando la diferencia entre el coste que para el operador designado tiene el operar con dichas obligaciones y el correspondiente a operar sin las mismas. El cálculo del coste neto tendrá en cuenta los beneficios, incluidos los beneficios no monetarios, que hayan revertido al operador designado.

2. No se incluirán en el cálculo del coste neto del servicio universal los costes sufridos como consecuencia de la prestación de cualquier servicio que, de acuerdo con lo establecido en este reglamento, quede fuera del ámbito de aplicación de las obligaciones de servicio universal.

3. Tendrán la consideración de servicios no rentables los solicitados por clientes o grupos de clientes, a los que un operador no se los prestaría a precio asequible, atendiendo a razones exclusivamente comerciales, bien por disfrutar de tarifas especiales, bien por su alto coste, incluido el de su acceso.

Son susceptibles de ser calificados como servicios no rentables los que deban prestarse a los usuarios que tengan discapacidades que impliquen una barrera de acceso al servicio o un uso más oneroso de este que el de un usuario sin discapacidad y a los colectivos de pensionistas y jubilados cuya renta familiar no exceda del indicador que, conforme al artículo 35.2.a).1.º, establezca la Comisión Delegada del Gobierno para Asuntos Económicos.

4. Al evaluar los costes en que incurre el operador por estar obligado a la prestación del servicio universal, se tendrá en cuenta una tasa razonable de remuneración de los capitales invertidos en su prestación, con referencia al coste del dinero en el mercado de capitales.

Artículo 40. *Componentes de coste neto del servicio universal.*

1. Los costes netos imputables a las obligaciones de servicio universal impuestas a los operadores que son susceptibles de compensación están compuestos por:

a) El coste neto de las obligaciones de suministrar la conexión a la red pública de comunicaciones electrónicas, desde una ubicación fija, a la que se refiere el artículo 28.1, con los plazos y las condiciones de razonabilidad establecidas en el artículo 29.

b) El coste neto de las obligaciones de prestar el servicio telefónico disponible al público, referidas en el artículo 28.2.

c) El coste neto de las obligaciones de prestar el servicio telefónico mediante teléfonos públicos de pago, referidas en el artículo 32.

d) El coste neto de la obligación de elaborar y poner a disposición de los abonados del servicio telefónico las guías telefónicas a las que se refiere el artículo 30.

e) El coste neto de las obligaciones de prestar los servicios de información números de abonados del servicio telefónico disponible al público, referidas en el artículo 31.

En todos los casos, dichas obligaciones se considerarán conjuntamente con las medidas para facilitar la accesibilidad que se establecen en el artículo 33, las condiciones de calidad del artículo 34 y las de asequibilidad del artículo 35, que le sean de aplicación.

2. La Comisión del Mercado de las Telecomunicaciones será el organismo encargado de definir y revisar la metodología para determinar el coste neto, tanto en lo que respecta a la imputación de costes como a la atribución de ingresos y deberá ser conforme con lo establecido en este reglamento y basarse en procedimientos y criterios objetivos, transparentes, no discriminatorios y proporcionales y tener carácter público.

3. Asimismo, la Comisión del Mercado de las Telecomunicaciones establecerá el procedimiento para cuantificar los beneficios no monetarios obtenidos por el operador, en su calidad de prestador de un servicio universal. En dicha valoración se tendrán en cuenta, como mínimo, las siguientes categorías de potenciales generadores de beneficios no monetarios:

a) Mayor reconocimiento de la marca del operador, como consecuencia de la prestación del servicio.

b) Ventajas derivadas de la ubicuidad.

c) Valoración de los clientes o grupos de clientes, teniendo en cuenta su ciclo de vida.

d) Ventajas comerciales que implica el tener acceso a todo tipo de datos sobre el servicio telefónico.

Artículo 41. *Coste neto de las obligaciones de suministrar la conexión a la red pública de comunicaciones electrónicas.*

1. El coste neto de las obligaciones de suministro de la conexión a la red pública de comunicaciones electrónicas se obtendrá sumando el coste neto asociado al suministro de las conexiones para la prestación eficiente de los servicios no rentables, referidos en el artículo 39,3, con el coste neto de suministrar las conexiones en las zonas no rentables, excluyendo posibles duplicidades, y deduciendo los beneficios, incluidos los beneficios no monetarios, debidos a la prestación de este elemento del servicio universal, obtenidos por su prestador.

2. El coste neto en las zonas no rentables se obtendrá hallando la diferencia entre los costes imputables debidos a su prestación eficiente y los ingresos atribuibles al suministro de las conexiones en dichas zonas que reviertan al prestador.

3. A los efectos de lo previsto en este artículo, se considerarán zonas no rentables las demarcaciones territoriales de prestación de conexiones a la red pública de comunicaciones electrónicas que un operador eficiente no cubriría a precio asequible, atendiendo a razones exclusivamente comerciales.

Artículo 42. *Coste neto de las obligaciones de prestar el servicio telefónico disponible al público.*

1. El coste neto de la obligación de prestación del servicio telefónico disponible al público se obtendrá sumando el coste neto asociado al servicio telefónico disponible al público para la prestación eficiente de los servicios no rentables, referidos en el artículo 39,3, con el coste neto de suministrar el servicio telefónico disponible al público en las zonas no rentables y deduciendo los beneficios, incluidos los beneficios no monetarios, debidos a la prestación de este elemento del servicio universal, obtenidos por el operador.

2. El coste neto en las zonas no rentables se obtendrá hallando la diferencia entre los costes imputables debidos a su prestación eficiente y los ingresos atribuibles al suministro del servicio telefónico disponible al público en dichas zonas que reviertan al prestador.

3. A los efectos de lo previsto en este artículo, se considerarán zonas no rentables las demarcaciones territoriales de prestación del servicio telefónico disponible al público que un operador eficiente no cubriría a precio asequible, atendiendo a razones exclusivamente comerciales.

Artículo 43. *Coste neto de las obligaciones relativas a las guías telefónicas y al servicio de consulta telefónica sobre números de abonado.*

1. El coste neto de la componente relativa a las guías telefónicas se obtendrá hallando la diferencia entre los costes imputables de su prestación eficiente y los ingresos atribuibles que reviertan al prestador, incrementando estos últimos con los beneficios, incluidos los beneficios no monetarios obtenidos por la prestación de este elemento del servicio universal.

2. El coste neto de la componente relativa a la obligación de prestar los servicios de consulta telefónica sobre números de abonados se obtendrá hallando la diferencia entre los costes imputables de su prestación eficiente y los ingresos atribuibles que reviertan al prestador, incrementando estos últimos con los beneficios, incluidos los beneficios no monetarios obtenidos por la prestación de este elemento del servicio universal.

Artículo 44. *Coste neto de las obligaciones relativas a los teléfonos públicos de pago.*

1. El coste neto de la obligación de asegurar la prestación del servicio de teléfonos públicos de pago en el dominio público de uso común en un determinado municipio se calculará hallando la diferencia entre los costes imputables soportados por el operador por

su instalación, mantenimiento, encaminamiento del tráfico saliente de aquellos y gestión eficiente, y los ingresos atribuibles generados por dichos teléfonos. Cuando el saldo así calculado muestre que en ese municipio los ingresos son superiores a los costes o cuando el número de estos teléfonos sea superior al exigido para cumplir con la oferta mínima referida en el artículo 32, y estos tengan una distribución territorial razonable, se considerará que no existe coste neto de la obligación en ese municipio.

2. El coste neto soportado por un operador designado para su prestación en una determinada zona geográfica, será el resultado de restar a la suma de los costes netos calculados para los municipios abarcados por dicha designación los beneficios, incluidos los beneficios no monetarios, obtenidos por la prestación de este elemento del servicio universal.

Artículo 45. *Determinación periódica del coste neto, verificación y aprobación administrativa.*

1. Los operadores con obligaciones de servicio universal, designados según el procedimiento previsto en el artículo 38, o según el previsto en el artículo 37 siempre que el coste neto efectivo no haya sido determinado en el proceso de designación, formularán anualmente una declaración a la Comisión del Mercado de las Telecomunicaciones de los servicios que ofrecen, cuya prestación sólo pueda hacerse con coste neto para ellos, detallando sus distintos componentes de costes e ingresos, de acuerdo con los principios y las normas de este reglamento y siguiendo las instrucciones que dicte la Comisión del Mercado de las Telecomunicaciones en ejercicio de sus facultades.

Para ello, el operador obligado, además de llevar una contabilidad separada que permita la adecuada asignación de los costes e ingresos, deberá encargar a una entidad cualificada e independiente, con una periodicidad anual, que compruebe dicha declaración de coste, y tendrá la obligación de aportar a la Comisión del Mercado de las Telecomunicaciones antes del 31 de julio del año siguiente el informe correspondiente que contenga una declaración de conformidad.

2. La cuantificación del coste neto contenida en dicha declaración deberá ser aprobada por la Comisión del Mercado de las Telecomunicaciones, previa verificación realizada por ella misma o por la entidad que, a estos efectos, designe. La Comisión del Mercado de las Telecomunicaciones publicará las conclusiones sobre el cumplimiento de los criterios de costes por parte de cada uno de los operadores obligados y la cuantificación del coste neto debidamente aprobada, con el límite de los aspectos confidenciales que puedan revelar una información contable excesivamente desagregada.

Artículo 46. *Determinación de la existencia de una carga injustificada.*

Cuando se haya apreciado un coste neto, la Comisión del Mercado de las Telecomunicaciones determinará, mediante resolución motivada, si dicho coste implica una carga injustificada para la empresa prestadora del servicio universal.

Sección 5.ª Financiación del servicio universal

Artículo 47. *Operadores obligados a financiar el servicio universal.*

1. Cuando, en virtud de lo establecido en el artículo 36.4, un operador designado tenga derecho a la financiación del coste neto que le supone la prestación del servicio universal, podrá instar el inicio del procedimiento para que la Comisión del Mercado de las Telecomunicaciones ponga en marcha el mecanismo de financiación para compartir dicho coste neto.

La Comisión del Mercado de las Telecomunicaciones publicará en el “Boletín Oficial del Estado” la lista de operadores obligados a contribuir, los datos referentes a dicho mecanismo y los principios aplicables al reparto de los costes.

2. La financiación del coste neto resultante de la obligación de prestación del servicio universal será compartida por todos los operadores de redes y servicios de comunicaciones electrónicas.

3. La Comisión del Mercado de las Telecomunicaciones podrá exonerar a determinados operadores de la obligación de contribuir a la financiación del servicio universal cuando su volumen de negocios a escala nacional se sitúe por debajo de un umbral preestablecido por ella.

La declaración de exención sólo tendrá efecto para el período que en ella se especifique, y el operador al que afecte deberá asumir la obligación de contribución al Fondo nacional de financiación del servicio universal una vez transcurrido, salvo que la Comisión del Mercado de las Telecomunicaciones expresamente lo prorrogue

Artículo 48. *Objetivos y principios de la financiación.*

1. El mecanismo de financiación garantizará unos incentivos adecuados que fomenten una prestación eficiente del servicio universal, y limitará los posibles efectos negativos sobre el mercado y las inversiones que puedan derivarse de unos costes más elevados de lo necesario.

2. Los objetivos del mecanismo de financiación del servicio universal son los siguientes:

a) Reducir al mínimo las barreras de acceso al mercado y garantizar al mismo tiempo la financiación del servicio universal.

b) Respetar el requisito de neutralidad entre operadores del mercado, las tecnologías específicas o la prestación de servicios, integrada o separadamente, para evitar una distorsión en las estrategias de acceso al mercado o, posteriormente, en las decisiones sobre inversión o en la actividad en dicho mercado.

c) Mantener al nivel mínimo las cargas administrativas y los costes relacionados con ellas.

d) Crear unas condiciones que propicien una mayor eficacia e innovación, para garantizar la prestación del servicio universal al menor coste posible.

3. El mecanismo de financiación respetará los principios generales de objetividad, proporcionalidad, no discriminación y transparencia.

4. En ningún caso, las aportaciones de un operador para la financiación del servicio universal darán lugar, directa o indirectamente, a que se duplique el pago destinado a sufragar el coste neto de una misma obligación de servicio universal específica.

Artículo 49. *Parámetros de reparto del coste neto entre los operadores obligados.*

1. Las aportaciones de los operadores de redes y servicios de comunicaciones electrónicas obligados a financiar el servicio universal serán proporcionales a la actividad de cada uno y serán determinadas por la Comisión del Mercado de las Telecomunicaciones.

El criterio de distribución se basará, para cada operador, en la cantidad resultante de detraer de los ingresos brutos de explotación los pagos mayoristas relacionados con la prestación de servicios incluidos en el ámbito del servicio universal y será proporcional al volumen total de negocio en el mercado.

2. El Ministerio de Industria, Turismo y Comercio, previo informe de la Comisión del Mercado de las Telecomunicaciones y en función de la evolución tecnológica y de las condiciones del mercado, podrá establecer otros parámetros de distribución que representen mejor la actividad de los operadores, a los efectos de un más equitativo reparto de la carga derivada del servicio universal.

3. Las aportaciones que los operadores designados para la prestación del servicio universal deban realizar al Fondo nacional de financiación del servicio universal, por estar obligados a financiar dicho servicio, serán minoradas en las cuantías que, en su caso, les corresponda percibir por las obligaciones de servicio universal que tengan impuestas.

La resultante podrá dar lugar a una aportación neta del operador al mecanismo de financiación o una recepción neta de subsidio.

Artículo 50. *Fondo nacional de financiación del servicio universal. Naturaleza y fines. Supresión del fondo.*

1. El Fondo nacional de financiación del servicio universal garantiza la financiación del servicio universal y recoge las aportaciones de los operadores obligados a contribuir a ella.

El fondo carece de personalidad jurídica propia y su gestión se llevará a cabo por la Comisión del Mercado de las Telecomunicaciones.

2. A través del fondo se persiguen los siguientes fines:

a) Gestionar el cobro efectivo de las aportaciones de los operadores de comunicaciones electrónicas.

b) Gestionar los pagos a los operadores con derecho a recibirlos por la prestación del servicio universal.

3. En relación con el fondo, la Comisión del Mercado de las Telecomunicaciones llevará a cabo las siguientes funciones:

a) Conocer su evolución económica y adoptar las medidas necesarias para el cumplimiento de sus fines.

b) Aprobar sus previsiones de ingresos y su liquidación anual.

c) Aprobar la memoria anual de su gestión que se incorporará al informe anual que ha de presentar conforme al procedimiento establecido en el artículo 20 de la Ley 2/2011 de Economía Sostenible.

d) Gestionar su patrimonio, cobro de derechos y atención de sus obligaciones.

e) Determinar las contribuciones de cada operador.

f) Resolver de forma vinculante los conflictos que se susciten entre operadores en materias relacionadas con el fondo.

4. En el caso de que el coste de la prestación del servicio universal para operadores sujetos a estas obligaciones sea de una magnitud tal que no justifique los costes derivados de la gestión del fondo, la Comisión del Mercado de las Telecomunicaciones podrá proponer al Gobierno su supresión y, en su caso, el establecimiento de mecanismos de compensación directa entre operadores.

Artículo 51. *Recursos del Fondo nacional de financiación del servicio universal. Aportaciones y gestión.*

1. Son recursos del Fondo nacional de financiación del servicio universal los siguientes:

a) Las aportaciones que realicen los operadores obligados a financiar el servicio universal.

b) Las aportaciones realizadas por cualquier otra persona física o jurídica que desee contribuir desinteresadamente a la financiación de cualquier actividad propia del servicio universal.

2. Las aportaciones pecuniarias se depositarán en una cuenta restringida abierta a tal efecto en una entidad de crédito. Al total de los activos se le deducirán los gastos de la gestión del fondo.

3. Los recursos del fondo sólo se podrán invertir en activos financieros de alta liquidez y rentabilidad asegurada.

4. El procedimiento para fijar las aportaciones y llevarlas a cabo será el siguiente:

a) En el plazo de dos meses a partir de la publicación de la lista referida en el artículo 47.1, cada operador obligado enviará la información relativa a sus ingresos del último ejercicio que se haya cerrado tres meses antes de la publicación de dicha lista a la Comisión del Mercado de las Telecomunicaciones.

b) La Comisión del Mercado de las Telecomunicaciones calculará las cuotas de mercado de los operadores obligados a contribuir y la aportación que les corresponda realizar a cada uno. En el plazo de dos meses, contados a partir de la finalización del plazo anterior relativo al envío de información sobre los ingresos, publicará en el «Boletín Oficial del Estado» la aportación anual que corresponda ingresar a cada operador obligado por este concepto y les requerirá para que efectúen los ingresos correspondientes, en un único pago en el plazo de un mes a partir de dicha notificación.

c) Los operadores con derecho a compensación la recibirán dentro del mes siguiente a la finalización del período de pago, de acuerdo con las aportaciones habidas.

5. Si un operador obligado a realizar aportaciones no las lleva a cabo en el plazo establecido, la deuda devengará un interés de demora igual al interés legal más dos puntos desde el día siguiente al de finalización del plazo de pago.

La Comisión del Mercado de las Telecomunicaciones podrá ejercer las acciones legales encaminadas al cobro de las cantidades debidas, y serán de cuenta del deudor los gastos que ello ocasione.

6. La obligación de prestar el servicio universal no quedará condicionada, en ningún caso, a la recepción de compensaciones que provengan del fondo.

7. La Comisión del Mercado de las Telecomunicaciones pondrá a disposición de los interesados, a solicitud de estos, la información disponible actualizada relativa a la gestión del Fondo nacional de financiación del servicio universal.

Artículo 52. *Costes de administración del fondo.*

Los costes de administración del fondo incluyen, al menos, los siguientes:

a) Los que ocasione al gestor la supervisión del coste neto.

b) Los administrativos.

c) Los derivados de la gestión de las contribuciones.

Dichos costes serán objeto de reparto entre los operadores obligados con los mismos criterios que el coste neto del servicio universal, formando parte de sus correspondientes aportaciones al fondo.

CAPÍTULO III

Otras obligaciones de servicio público

Artículo 53. *Obligaciones de servicio público previstas en el apartado 1 del artículo 25 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

El Gobierno, mediante acuerdo del Consejo de Ministros, podrá imponer obligaciones de servicio público distintas del servicio universal por necesidades de la defensa nacional, de la seguridad pública o de la seguridad de las personas o de protección civil.

El acuerdo del Consejo de Ministros que imponga dichas obligaciones establecerá, asimismo, la forma de gestión, directa o indirecta, del servicio y el sometimiento, en su caso, a los principios generales establecidos en el artículo 26.

Artículo 54. *Obligaciones de servicio público previstas en el apartado 2 del artículo 25 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La inclusión de nuevos servicios que comporten la acreditación fehaciente del contenido del mensaje o de su remisión o recepción distintos de los encomendados inicialmente a la Sociedad Estatal Correos y Telégrafos, S. A., así como la designación de la entidad encargada de prestarlos, se efectuará por acuerdo del Consejo de Ministros.

El Gobierno, previo informe de la Comisión del Mercado de las Telecomunicaciones, podrá imponer otras obligaciones de servicio público motivadas por las necesidades o razones previstas en dicho apartado, así como establecer su forma de financiación.

La inclusión entre los servicios encomendados a la Sociedad Estatal Correos y Telégrafos, S. A., de otros de contenido similar, que comporten la acreditación fehaciente del contenido del mensaje o de su remisión o recepción, sus características técnicas, las de su prestación y las de financiación, se efectuarán, en su caso por orden del Ministerio de la Presidencia, a propuesta de los Ministerios de Industria, Turismo y Comercio y de Fomento.

Serán de aplicación a los servicios regulados en este artículo los principios generales establecidos en el artículo 26.

Artículo 55. *Principios aplicables para la determinación de los operadores obligados a cumplir las obligaciones de servicio público previstas en este capítulo.*

El real decreto o, en su caso, el acuerdo del Consejo de Ministros que establezca obligaciones de servicio público subsumibles en alguno de los artículos de este capítulo y

distintas de las inicialmente fijadas en la disposición transitoria cuarta de este reglamento establecerá lo siguiente:

a) La forma de designación del operador obligado, tomando en consideración los principios aplicables fijados en el artículo 26 y previendo, cuando proceda, un procedimiento de selección competitiva.

b) La definición de los objetivos que se prevén alcanzar.

c) La delimitación de la cobertura y áreas territoriales prioritarias y, en su caso, de las demarcaciones para la prestación de los servicios.

d) La fijación, en su caso, de los parámetros para la determinación del carácter asequible de los precios y de los mecanismos para su medición y control.

e) La forma de financiación de las obligaciones de servicio público y programa de asignación de fondos para alcanzar los objetivos.

f) El calendario de actuaciones o, en su caso, criterios para el establecimiento de prioridades.

Artículo 56. *Obligaciones de servicio público en materia de transmisión de determinados canales y servicios de programas de radiodifusión y televisión.*

1. Sin perjuicio de las obligaciones que los operadores tengan impuestas en virtud de lo establecido en la normativa de acceso e interconexión, de lo dispuesto en el capítulo III del título II de este reglamento, de las obligaciones impuestas por razón de la interoperabilidad de los servicios o de las impuestas en materia de regulación de los mercados de referencia, tendrán la consideración de obligaciones de servicio público del artículo 25.2.b) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, las establecidas en el apartado 4 de la disposición adicional séptima de la citada ley y las de cobertura y calidad exigibles a las personas físicas o jurídicas que tengan títulos habilitantes de radiodifusión o televisión que sustituyan las previstas en la disposición transitoria sexta de dicha ley. A estos efectos, los operadores de redes públicas de comunicaciones electrónicas estarán obligados a cumplir las exigencias de transmisión de determinados canales y servicios de programas de radio y televisión o de cobertura y calidad que se establezcan de conformidad con este artículo.

2. Para la imposición de las obligaciones de servicio público a que se refiere el apartado anterior, deberán cumplirse los siguientes requisitos:

a) Que los operadores a los que se imponga la obligación exploten redes de comunicaciones electrónicas utilizadas para la distribución de programas de radio o televisión al público.

b) Que un número significativo de usuarios finales de dichas redes las utilice como medio principal de recepción de programas de radio y televisión.

c) Que la imposición como obligación de servicio público sea necesaria para alcanzar objetivos de interés general claramente definidos por la legislación básica en materia de medios de comunicación social.

d) Que se cumplan los principios generales aplicables para la imposición de obligaciones de servicio público establecidas en el artículo 26.

3. Los operadores en los que concurran los requisitos establecidos en los párrafos a) y b) del apartado anterior tendrán la obligación de facilitar sus capacidades de transmisión y de red a las personas físicas o jurídicas que tengan los títulos habilitantes de radiodifusión o televisión a las que, en aplicación de la legislación básica del Estado dictada al amparo de su competencia en materia de medios de comunicación social, prevista en el artículo 149.1.27.ª de la Constitución, se reconozcan derechos de distribución de determinados canales y servicios de programas de radio y televisión, o a las que se impongan obligaciones en materia de cobertura y calidad. Dicha legislación básica deberá determinar claramente el tipo de financiación que, en su caso, se prevea, los sujetos beneficiarios u obligados y justificar debidamente la concurrencia de los requisitos establecidos en los párrafos c) y d) del apartado anterior.

4. Cuando la legislación básica sobre medios de comunicación social no determine el tipo de financiación, la retribución que, en su caso, proceda a los operadores de comunicaciones electrónicas obligados en virtud de este artículo como compensación por la

imposición de las obligaciones de servicio público previstas en él deberá ser acordada libremente entre ellos y las personas físicas o jurídicas que tengan los correspondientes títulos habilitantes de radiodifusión o televisión a los que correspondan, respectivamente, los derechos de distribución de determinados canales y servicios de programas de radio y televisión o las obligaciones en materia de cobertura y calidad. En caso de desacuerdo sobre las condiciones técnicas y económicas aplicables, corresponderá a la Comisión del Mercado de las Telecomunicaciones resolver el conflicto mediante resolución vinculante, previa solicitud de alguna de las partes y previa tramitación de expediente contradictorio.

TÍTULO IV

Derecho de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y condiciones de establecimiento de servidumbres y limitaciones

Artículo 57. *Derecho a la ocupación del dominio público y a ser beneficiario en expedientes de expropiación forzosa.*

Los operadores tendrán derecho, en la medida en que sea necesario para el establecimiento de una red pública de comunicaciones electrónicas y en los términos establecidos en el capítulo II del título III de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, a la ocupación del dominio público y de la propiedad privada.

Los operadores, para el ejercicio de dichos derechos, estarán obligados a cumplir las condiciones exigibles que se establecen en este reglamento y, en concreto, las normas que se fijen por las Administraciones públicas competentes de conformidad con lo dispuesto en los artículos 28 y 29 de la Ley 32/2003, de 3 de noviembre, y con sujeción a los límites de emisión que se establezcan en desarrollo de lo previsto en el artículo 44.1.a) de dicha ley.

Artículo 58. *Derecho a ser beneficiarios en el procedimiento de expropiación forzosa.*

1. Los operadores, cuando resulte estrictamente necesario para la instalación de la red, en la medida prevista en el proyecto técnico presentado y siempre que no existan otras alternativas económicamente viables, tendrán derecho a la ocupación de la propiedad privada, ya sea a través de su expropiación forzosa, ya sea mediante la declaración de servidumbre forzosa de paso para la instalación de infraestructuras de redes públicas de comunicaciones electrónicas. A dichos efectos, podrán solicitar ser beneficiarios en un expediente concreto, siempre que cumplan lo dispuesto en la Ley 32/2003, de 3 de noviembre, y en la normativa vigente en materia de expropiación forzosa.

2. La aprobación del proyecto técnico por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información llevará implícita, en cada caso concreto, la declaración de utilidad pública y la necesidad de ocupación para la instalación de redes públicas de comunicaciones electrónicas, a los efectos de lo previsto en la legislación de expropiación forzosa.

3. Con carácter previo a la aprobación del proyecto técnico, se recabará informe de la comunidad autónoma competente, de conformidad con lo dispuesto en el artículo 27 de la Ley 32/2003, de 3 de noviembre.

4. En las expropiaciones que se lleven a cabo para la instalación de redes públicas de comunicaciones electrónicas cuyos titulares tengan impuestas obligaciones de servicio público indicadas en el artículo 22 o en los apartados 1 y 2 del artículo 25 de la Ley 32/2003, de 3 de noviembre, se seguirá el procedimiento especial de urgencia establecido en la Ley de Expropiación Forzosa, cuando así se haga constar en la resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información que apruebe el oportuno proyecto técnico.

Artículo 59. *Uso compartido del dominio público y privado para la instalación de infraestructuras.*

1. Las Administraciones públicas competentes podrán fomentar el uso compartido del dominio público o de la propiedad privada para el establecimiento de redes públicas de comunicaciones electrónicas.

Asimismo, en los términos establecidos en el artículo 30 de la Ley 32/2003, de 3 de noviembre, las Administraciones públicas podrán acordar que, desde la fecha en que se dicte la correspondiente resolución, el dominio público o la propiedad privada estarán sujetos al régimen de uso compartido previsto en dicho artículo.

El uso compartido se articulará mediante acuerdos entre los operadores interesados. En el caso de ocupación del dominio público, a falta de acuerdo en el plazo de un mes, cualquiera de los operadores podrá, previa comunicación al resto de ellos y al titular de dicho dominio, requerir a la Comisión del Mercado de las Telecomunicaciones para que emita el informe previsto en el artículo 30.3 de la Ley 32/2003, de 3 de noviembre.

2. No obstante lo dispuesto en el apartado anterior, las condiciones para el uso compartido de los locales e infraestructuras de comunicaciones electrónicas para la interconexión de redes publicas de comunicaciones electrónicas se sujetarán a lo dispuesto en el reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en materia de interconexión, y quedarán excluidas de la aplicación de lo dispuesto en este artículo.

3. Cuando en aplicación de los límites de emisión que se fijen de conformidad con lo dispuesto en el artículo 44.1.a) de la Ley 32/2003, de 3 de noviembre, se establezcan límites en los niveles de emisión para el uso compartido de infraestructuras, deberán autorizarse más emplazamientos para asegurar la cobertura en los términos establecidos en el artículo 30.4 de dicha ley.

Artículo 60. *Otras servidumbres y limitaciones.*

1. Los operadores, en la medida en que sea necesario para la protección de sus redes públicas de comunicaciones electrónicas, podrán obtener la protección del dominio público radioeléctrico que utilicen para dichas redes, para lo que solicitarán la imposición de servidumbres y limitaciones a la propiedad, de conformidad con lo dispuesto en la disposición adicional primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. En los términos que se establezcan en la normativa reglamentaria que desarrolle el artículo 44 de la Ley 32/2003, de 3 de noviembre, podrán fijarse, de conformidad con lo previsto en el artículo 32.2 de dicha ley, límites al derecho de uso del dominio público radioeléctrico para la protección de otros bienes jurídicamente protegidos prevalentes.

TÍTULO V

Obligaciones de carácter público. Secreto de las comunicaciones y protección de los datos personales

CAPÍTULO I

Protección de los datos personales en la explotación de redes y en la prestación de los servicios de comunicaciones electrónicas disponibles al público

Sección 1.ª Disposiciones generales

Artículo 61. *Ámbito de aplicación.*

1. Este capítulo tiene por objeto el establecimiento de las normas reglamentarias de carácter técnico de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en relación con la protección de los datos personales en la explotación de redes y en la prestación de los servicios de comunicaciones electrónicas disponibles al

público. Lo regulado en este capítulo es de aplicación al tratamiento de los datos personales en la prestación de servicios de comunicaciones electrónicas disponibles al público y en la explotación de redes públicas de comunicaciones electrónicas, así como en las actividades que realicen los sujetos a los que se refiere el artículo 51.c) de la Ley 32/2003, de 3 de noviembre, en los supuestos en que este resulte de aplicación.

2. Las disposiciones sobre visualización y limitación de la identificación de la línea de origen y de la línea conectada y sobre el desvío automático de llamadas se aplicarán, en los términos establecidos en la sección 3.ª de este capítulo, a las líneas de abonados conectadas a centrales digitales y, cuando sea técnicamente posible y no exija una inversión desproporcionada por el operador, a las líneas de abonados conectadas a centrales analógicas. Los operadores deberán obtener del Ministerio de Industria, Turismo y Comercio la autorización correspondiente para quedar exentos del cumplimiento de los requisitos sobre visualización y limitación de la identificación de la línea de origen y conectada y sobre desvío automático de llamadas.

3. No será de aplicación lo establecido en este capítulo cuando, de conformidad con la normativa vigente, sea necesario adoptar medidas para la protección de la seguridad pública, la seguridad del Estado, la aplicación del derecho penal y la interceptación legal de las comunicaciones electrónicas para cualesquiera de estos fines.

Artículo 62. *Protección y seguridad de los datos personales.*

1. Los sujetos obligados a los que se refiere el artículo 51 de la Ley 32/2003, de 3 de noviembre, deberán garantizar la protección de los datos personales en el ejercicio de su actividad, en los términos establecidos en este reglamento y en la legislación vigente.

2. Los operadores deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, para garantizar los niveles de protección de los datos de carácter personal establecidos en este reglamento y demás normativa aplicable.

En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y, cuando el riesgo quede fuera del ámbito de las medidas que deberá tomar el prestador del servicio, sobre las posibles soluciones, con una indicación de los posibles costes.

Artículo 63. *Régimen jurídico.*

La protección de los datos personales vinculados a las redes y servicios de comunicaciones electrónicas se regirá por lo dispuesto en el artículo 38 de la Ley 32/2003, de 3 de noviembre, por este título V y, en lo no previsto por aquellas normas, por lo dispuesto en legislación vigente sobre protección de los datos de carácter personal.

Artículo 64. *Definiciones.*

A los efectos de este título, se entiende por:

a) Datos de tráfico: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación.

b) Datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.

c) Comunicación: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información.

d) Llamada: una conexión establecida por medio de un servicio telefónico disponible para el público que permita la comunicación bidireccional en tiempo real.

e) Servicio con valor añadido: todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vaya más allá de lo necesario para la transmisión de una comunicación o su facturación.

f) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

g) Facilidad de identificación de la línea de origen: la prestación que permite que el usuario que recibe una llamada, obtenga la información del número telefónico de la línea desde donde se origina esa comunicación.

h) Facilidad de identificación de línea conectada: la prestación que permite que el usuario que origina la llamada obtenga información del número telefónico de la línea a la que ha sido conectada su llamada.

Sección 2.ª Los datos de carácter personal en relación con determinados aspectos de los servicios de comunicaciones electrónicas

Artículo 65. *Datos personales sobre el tráfico y la facturación.*

1. Los operadores deberán eliminar o hacer anónimos los datos de carácter personal sobre el tráfico referidos a una comunicación y relacionados con los usuarios y los abonados que hayan sido tratados y almacenados para establecer una comunicación, en cuanto ya no sean necesarios a los efectos de su transmisión, sin perjuicio de lo dispuesto en los apartados siguientes.

2. Los datos de tráfico que fueran necesarios para realizar la facturación y los pagos de las interconexiones podrán ser tratados únicamente durante el plazo en que pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable. Transcurrido dicho plazo, los operadores deberán eliminar o hacer anónimos los datos de carácter personal, en los términos del apartado 1.

3. Asimismo, los operadores podrán tratar los datos de tráfico con fines de promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido, en la medida y durante el tiempo necesarios para la prestación de tales servicios o su promoción comercial, siempre y cuando el abonado haya dado su consentimiento informado.

A estos efectos, los sujetos obligados deberán dirigirse a los abonados, al menos, con un mes de antelación al inicio de la promoción o de la prestación del servicio con valor añadido, informarles del tipo de servicios para los que se efectuará el tratamiento, los tipos de datos que serán objeto de tratamiento y la duración que tendrá y solicitarles su consentimiento para el tratamiento de los datos. Esta comunicación, que deberá efectuarse a través de un medio que garantice su recepción por parte del abonado, podrá llevarse a cabo de forma conjunta a la facturación del servicio prestado por los sujetos obligados al abonado.

Deberá facilitarse al interesado un medio sencillo y que no implique ingreso alguno para el sujeto obligado para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado a este reglamento el procedimiento en el que tal negativa pueda efectuarse mediante un envío prefranqueado al sujeto obligado o la llamada a un número telefónico gratuito o a los servicios de atención al cliente que aquel hubiera establecido.

Si en el plazo de un mes desde que el abonado reciba la solicitud este no se hubiese pronunciado al respecto, se entenderá que consiente el tratamiento de los datos de tráfico para esta finalidad, siempre que así se hubiera hecho constar en la información dirigida al abonado.

En todo caso, los abonados dispondrán de la posibilidad de retirar en cualquier momento su consentimiento para el tratamiento de sus datos de tráfico al que se refiere este apartado.

4. El operador deberá informar al abonado o al usuario de los tipos de datos de tráfico que son tratados y de la duración de este tratamiento a los efectos mencionados en el apartado 2 y, antes de obtener el consentimiento, a los efectos previstos en el apartado 3.

5. El tratamiento de los datos de tráfico, de conformidad con los apartados anteriores, sólo podrá realizarse por las personas que actúen bajo la autoridad del operador prestador del servicio o explotador de la red que se ocupen de la facturación o de la gestión del tráfico,

de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas, de la prestación de un servicio con valor añadido o de suministrar la información requerida por los jueces y tribunales, por el Ministerio Fiscal o por los órganos o entidades que pudieran reclamarla en virtud de las competencias atribuidas por la Ley 32/2003, de 3 de noviembre.

En todo caso, dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.

Artículo 66. *Protección de los datos personales en la facturación desglosada.*

Los abonados tendrán derecho a recibir facturas no desglosadas cuando así lo soliciten a los operadores que, de conformidad con lo dispuesto en este reglamento, tengan la obligación de prestar dicho servicio.

Asimismo, por resolución del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, se fijarán las distintas modalidades de presentación de la facturación desglosada que los abonados pueden solicitar a los operadores, tales como la supresión de un determinado número de cifras en la factura de los números a los que se ha llamado o la no aparición en la factura de los números a los que se llama cuando el pago se haga con tarjeta de crédito, como mecanismos de garantía de la utilización anónima o estrictamente privada del servicio.

Las llamadas que tengan carácter gratuito para el abonado que efectúa la llamada, incluidas las llamadas a los números de asistencia, no figurarán en las facturas detalladas del abonado que efectúa la llamada.

Artículo 67. *Guías de servicios de comunicaciones electrónicas disponibles al público.*

1. Los sujetos obligados deberán informar gratuitamente a sus abonados antes de incluir o facilitar sus datos a otra entidad con destino a su inclusión en cualquier tipo de guía de abonados, impresa o electrónica, disponible al público o accesible a través de servicios de información o de consulta sobre ella, de la finalidad de dicha guía, así como de cualquier otra posibilidad de uso basada en funciones de búsqueda incorporadas en sus versiones electrónicas. Dicha información a los abonados deberá producirse al menos con un mes de antelación a que los datos sean incluidos o facilitados a otra entidad para su inclusión, y se les deberá solicitar su consentimiento, en los términos establecidos en los apartados siguientes.

2. Para que los datos correspondientes a un abonado a los que se refiere el artículo 30.4 sean incluidos por primera vez en algún tipo de guía o facilitados a otra entidad para su inclusión en ella o para la prestación de servicios de información o de consulta sobre ella, será preciso el consentimiento expreso de dicho abonado. A estos efectos, se entenderá que existe consentimiento expreso de un abonado cuando el operador le solicite su consentimiento para la inclusión de tales datos, con indicación expresa de cuáles serán estos, el modo en que serán incluidos en la guía y su finalidad, y este le responda dando su aceptación. También se producirá cuando este se dirija por escrito a su operador solicitándole que sus datos figuren en la guía.

Si el abonado no hubiese dado su consentimiento expreso, se entenderá que no acepta que se publiquen en la guía correspondiente sus datos.

Una vez otorgado el consentimiento conforme al párrafo anterior, para las sucesivas inclusiones de dichos datos en la guía o su entrega a otra entidad para su inclusión en ella o para la prestación de servicios de información o de consulta sobre ella, bastará con que, en el plazo de un mes, en la comunicación en la que se solicita el consentimiento, el abonado no se oponga expresamente a dicha inclusión.

3. La inclusión en una guía, impresa o electrónica, de cualquier dato distinto de los previstos en el artículo 30.4 exigirá el consentimiento expreso del abonado para ello, tanto la primera vez como las sucesivas inclusiones.

A estos efectos, se entenderá que existe consentimiento expreso de un abonado cuando este se dirija por escrito a quien elabora la guía o a quien facilita sus datos personales a otra entidad con esa finalidad y le solicite que amplíe sus datos personales que figuran en la guía. También se producirá cuando quien elabora la guía o a quien facilita sus datos personales a otra entidad con esa finalidad solicite al abonado su consentimiento para la

inclusión de tales datos, indicando expresamente cuáles serán estos, el modo en que serán incluidos en la guía y su finalidad, y este le responda dando su aceptación.

Si el abonado no hubiese dado su consentimiento expreso, se entenderá que no acepta que se publiquen en la guía correspondiente otros datos que no sean los que se establecen en el párrafo primero de este apartado.

4. Los abonados tendrán derecho a que sus datos que aparezcan en la guía no sean utilizados con fines de publicidad o prospección comercial y a que así conste de forma clara en la guía. Del mismo modo tendrán derecho a que se omita parcialmente su dirección o algún otro dato, en los términos que haya estipulado su proveedor. Asimismo, podrán ejercer los derechos de acceso, rectificación, cancelación y oposición, en los términos previstos en la legislación vigente en materia de protección de datos de carácter personal.

El ejercicio de los derechos a los que se refiere este apartado no deberá implicar ingreso alguno para el sujeto obligado.

Los abonados que hayan ejercido su derecho a no figurar en las guías tendrán derecho a recibir la información adicional a la que se refiere el párrafo primero del apartado 2 del artículo 71.

5. La guía a la que se refiere el artículo 30 dejará de tener el carácter de fuente accesible al público cuando se publique la siguiente actualización. El resto de guías perderán dicho carácter con la siguiente actualización o, en su defecto, tras el transcurso del plazo de un año desde su última publicación, con independencia del formato en que se hayan elaborado.

6. Lo dispuesto en los apartados anteriores en relación con las guías de abonados será de aplicación a los datos utilizados para la prestación de servicios de consulta sobre números de abonado.

Artículo 68. *Prestación de los servicios de elaboración de guías de abonados y de consulta telefónica sobre números de abonado.*

1. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de servicios de consulta telefónica sobre números de abonado se realizará en régimen de libre competencia.

2. La Comisión del Mercado de las Telecomunicaciones deberá suministrar gratuitamente a las entidades que vayan a elaborar guías telefónicas de abonados, a las que presten el servicio de consulta telefónica sobre números de abonado y a las que presten los servicios de llamadas de emergencia, los datos que le faciliten los operadores, de conformidad con lo establecido en este reglamento, con las instrucciones que, en su caso, dicte la Comisión del Mercado de las Telecomunicaciones y con lo que a tal efecto se establezca por orden ministerial.

Los datos referentes a los abonados que hubieran ejercido su derecho a no figurar en las guías accesibles al público únicamente se proporcionarán a las entidades titulares del servicio de atención de llamadas de emergencia. A estos efectos, se entenderá que los servicios de llamadas de emergencia son los prestados a través del número 112 y aquellos otros que determine la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

El suministro se realizará a solicitud expresa de la entidad interesada y previa resolución motivada de la Comisión del Mercado de las Telecomunicaciones, previo informe de la Agencia Española de Protección de Datos, en la que se reconozca que la entidad reúne los requisitos para acceder a los datos y se establezcan las condiciones de suministro y de utilización de los datos suministrados.

3. Las entidades que reciban los datos de la Comisión del Mercado de las Telecomunicaciones estarán obligadas a la prestación de los servicios que motivan la comunicación de los datos, a la utilización de los datos comunicados única y exclusivamente para dicha prestación y a la utilización para ello de la última versión actualizada de los datos que se encuentre disponible.

En caso de que en el plazo de seis meses desde el reconocimiento del derecho de la entidad solicitante al acceso a los datos del abonado esta no hubiera iniciado la prestación de los servicios en virtud de los cuales se acordó el suministro de la información, o se comprobase que con posterioridad al reconocimiento del derecho los datos se utilizan para otras finalidades distintas o son empleados de forma distinta a la establecida por la Comisión

del Mercado de las Telecomunicaciones, esta, previo informe de la Agencia Española de Protección de Datos, dictará una resolución motivada que revoque, en su caso, la resolución por la que se reconoció el derecho de acceso a los datos.

Si se acordase la revocación de la resolución por la que se reconoció el derecho de acceso a los datos, la entidad interesada deberá proceder a la supresión inmediata de los datos que le hubieran sido comunicados, así como cualquier copia de estos.

Lo establecido en este apartado se entiende sin perjuicio de las competencias atribuidas a la Agencia Española de Protección de Datos por la legislación vigente en materia de protección de datos de carácter personal.

Artículo 69. *Llamadas no solicitadas para fines de venta directa.*

1. Las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas de llamada automática, a través de servicios de comunicaciones electrónicas, sin intervención humana (aparatos de llamada automática) o facsímil (fax), sólo podrán realizarse a aquellos que hayan dado su consentimiento previo, expreso e informado.

El incumplimiento de lo establecido en el párrafo anterior será sancionado de acuerdo con lo establecido en el artículo 38.3.c), o en el artículo 38.4.d) de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

2. Las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas distintos de los establecidos en el apartado anterior podrán efectuarse salvo las dirigidas a aquellos que hayan manifestado su deseo de no recibir dichas llamadas.

No obstante lo dispuesto en el párrafo anterior, para realizar las llamadas a las que este se refiere a quienes hubiesen decidido no figurar en las guías de comunicaciones electrónicas disponibles al público o a los que hubiesen ejercido su derecho a que los datos que aparecen en ellas no sean utilizados con fines de publicidad o prospección comercial, será preciso contar con el consentimiento expreso de aquéllos.

Artículo 70. *Datos de localización distintos de los datos de tráfico.*

1. En el caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento expreso de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido.

A estos efectos, los sujetos obligados deberán dirigirse a los usuarios o abonados, al menos, con un mes de antelación al inicio de la prestación del servicio con valor añadido, e informarles del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a los efectos de la prestación del servicio con valor añadido, y solicitarles su consentimiento para el tratamiento de los datos. Esta comunicación, que deberá efectuarse por un medio que garantice su recepción por el usuario o abonado, podrá llevarse a cabo de forma conjunta a la facturación del servicio prestado por los sujetos obligados al abonado.

Se entenderá que existe consentimiento expreso cuando el usuario o el abonado se dirijan al sujeto obligado y le soliciten la prestación de los servicios con valor añadido que exijan el tratamiento de sus datos de localización.

En todo caso, los usuarios o abonados deberán contar con la posibilidad de retirar en cualquier momento su consentimiento para el tratamiento de sus datos de localización distintos de los de tráfico al que se refiere este apartado, así como de rechazar temporalmente el tratamiento de tales datos, mediante un procedimiento sencillo y gratuito, para cada conexión a la red o para cada transmisión de una comunicación.

2. Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

3. Sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico de conformidad con los apartados 1 y 2 las personas que actúen bajo la autoridad

del operador de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.

4. No obstante lo dispuesto en este artículo, los operadores facilitarán los datos de localización distintos a los datos de tráfico a las entidades autorizadas para la atención de las de urgencia, cuando el destino de las llamadas corresponda a tales entidades.

Sección 3.ª Protección de los datos personales en los servicios avanzados de telefonía

Artículo 71. *Visualización y restricción de la línea de origen y conectada.*

1. Lo establecido en este capítulo será de aplicación a los operadores que presten servicios telefónicos disponibles al público con las facilidades de identificación de la línea de origen e identificación de la línea conectada.

2. Los operadores citados en el apartado 1 informarán individualmente a cada uno de sus abonados, con 15 días de antelación al inicio de la prestación de las facilidades de identificación de la línea de origen y de la línea conectada, de las características de dichas facilidades. En particular, en la información dirigida a los abonados que hubieran decidido no aparecer en las guías, poniéndose de manifiesto la especial situación del abonado, deberá detallarse el modo en que la utilización de las mencionadas facilidades puede afectar a la protección de su intimidad y a su derecho a la protección de sus datos de carácter personal.

Los operadores deberán someter la comunicación que vayan a utilizar para informar a los abonados a informe de la Agencia Española de Protección de Datos.

Los operadores ofrecerán a los abonados un servicio de atención rápido y gratuito para que puedan realizar consultas sobre el funcionamiento de estas facilidades y para que comuniquen, en su caso, la configuración y opciones elegidas para éstas.

Los operadores que vayan a prestar las facilidades de identificación de la línea de origen o de la línea conectada deberán remitir al Ministerio de Industria, Turismo y Comercio y a la Agencia Española de Protección de Datos, con carácter previo a la prestación de estas facilidades, un documento que recoja las características y los procedimientos empleados para garantizar el cumplimiento de lo establecido en este reglamento sobre dichas facilidades. Asimismo, los operadores tendrán obligación de comunicar, de manera previa a su aplicación, las posteriores variaciones de las características de sus ofertas.

Artículo 72. *Supresión en origen, llamada a llamada, de la identificación de la línea de origen.*

Los operadores citados en el apartado 1 del artículo anterior que intervengan en el establecimiento de comunicaciones con la facilidad de identificación de la línea de origen deberán, necesariamente, ofrecer la posibilidad, en el tramo de red correspondiente, de que el usuario que origine las llamadas pueda suprimir, en cada una de ellas y mediante un procedimiento sencillo y gratuito, la identificación de la línea de origen.

La supresión en origen por el usuario, llamada a llamada, de la identificación de la línea de origen en las redes telefónicas públicas fijas se realizará mediante la marcación de un código en los accesos telefónicos que se realicen a través de estas redes.

A los efectos de lo establecido en el párrafo anterior, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información atribuirá un número corto como código para la supresión en origen por el usuario, llamada a llamada, de la identificación de la línea de origen.

La supresión en origen por el usuario, llamada a llamada, de la identificación de la línea de origen en las redes de telefonía móvil, en su modalidad GSM y en la red digital de servicios integrados deberá realizarse mediante la marcación de códigos que se ajusten, por orden de preferencia, a la normativa técnica europea, a la normativa internacional, a los acuerdos internacionales de operadores y, en su defecto o de manera complementaria, a las especificaciones técnicas nacionales.

La marcación de los códigos mencionados en los párrafos anteriores deberá realizarse de manera previa al de selección de operador, en su caso, y al número del abonado destinatario de la llamada.

No obstante lo anterior, la prestación de la telefonía rural de acceso celular basada en tecnología analógica no estará sujeta a la obligación establecida en este artículo.

Artículo 73. *Supresión en origen por línea de la identificación de la línea de origen.*

Los operadores citados en el apartado 1 del artículo 71, que intervengan en el establecimiento de comunicaciones con la facilidad de identificación de la línea de origen, deberán necesariamente ofrecer la posibilidad, en la medida en que cooperen en el establecimiento de dichas comunicaciones, de que cualquier abonado pueda suprimir de forma automática en todas sus llamadas la identificación de su línea.

Los abonados podrán, de manera gratuita, activar o desactivar dicha supresión automática dos veces en los seis meses siguientes al inicio del suministro de información referida en el apartado 3 del artículo 71. Posteriormente, el abonado podrá, de manera gratuita, realizar dicha operación una vez por cada período de seis meses. Para las activaciones o desactivaciones más frecuentes, los operadores podrán establecer un precio, orientado a costes. Los operadores no podrán establecer cuotas periódicas o precios por otros conceptos distintos de este último en la prestación de la supresión automática de la identificación de la línea de origen.

Artículo 74. *Código de selección de operador.*

Cuando en el establecimiento de una comunicación se haya realizado una selección de operador mediante la marcación de código, éste no deberá visualizarse en destino.

Artículo 75. *Supresión en destino de la identificación de la línea de origen.*

Cuando los operadores citados en el apartado 1 del artículo 71 ofrezcan en destino la identificación de la línea de origen, deberán ofrecer al abonado que recibe la llamada la posibilidad, mediante un procedimiento sencillo y gratuito, de impedir la visualización de la identificación de la línea de origen en las llamadas recibidas.

Los abonados podrán, de manera gratuita, activar o desactivar la supresión de la visualización en destino de la línea de origen dos veces en los seis meses siguientes al inicio del suministro de información referida en el apartado 3 del artículo 71. Posteriormente, el abonado podrá, de manera gratuita, realizar dicha operación una vez por cada período de seis meses. Para las activaciones o desactivaciones más frecuentes, los operadores podrán establecer un precio, orientado a costes. Los operadores no podrán establecer cuotas periódicas o precios por otros conceptos distintos de este último en la prestación de la supresión automática de la identificación en destino de la línea de origen.

Artículo 76. *Filtrado en destino de llamadas sin identificación.*

Cuando los operadores citados en el apartado 1 del artículo 71 ofrezcan en destino la identificación de la línea de origen y ésta se presente con anterioridad a que se establezca la llamada, deberán ofrecer al abonado que recibe la llamada la posibilidad, mediante un procedimiento sencillo, de rechazar las llamadas procedentes de usuarios o abonados que hayan impedido la visualización de la identificación de la línea de origen.

Artículo 77. *Eliminación de la supresión en origen de la identificación de línea de origen.*

Los operadores citados en el apartado 1 del artículo 71 eliminarán las marcas de supresión en origen de la identificación de la línea de origen, cuando el destino de las llamadas corresponda a entidades que presten servicios de llamadas de urgencias a través del número 112 y otras autorizadas para la atención de las de emergencia o a las relacionadas con la seguridad pública o la defensa nacional. La aplicación del mecanismo de eliminación de marcas de supresión en origen de la identificación de la línea de origen para servicios de emergencias distintos de los atendidos a través del número 112 deberá ser aprobada, a solicitud de las entidades prestadoras de los citados servicios de emergencia o

de oficio, de manera previa y para cada caso particular o tipo de servicio de emergencia, mediante resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

La aplicación del mecanismo de eliminación de marcas de supresión en origen de la identificación de la línea de origen por motivos de seguridad pública o defensa nacional se realizará cuando así lo establezca por resolución el Ministerio competente en dichas materias. La resolución se tramitará y aprobará siguiendo los principios de transparencia y proporcionalidad, y será comunicada a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y al resto de Autoridades de Reglamentación a que se refiere el artículo 46 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Asimismo, se podrán eliminar por un período de tiempo limitado las marcas de supresión en origen de la identificación de la línea de origen cuando el abonado haya solicitado la identificación de las llamadas maliciosas o molestas, de acuerdo con lo establecido en la normativa vigente en cada momento sobre protección y suspensión de las garantías del secreto de las comunicaciones.

Artículo 78. *Supresión permanente en destino de la identidad de la línea de origen.*

El Ministerio de Industria, Turismo y Comercio podrá establecer, para proteger los derechos de los ciudadanos, en especial el derecho a la intimidad, que, de manera gratuita, ciertos destinos de las llamadas asociados a determinados servicios no dispongan de la facilidad de identificación de la línea de origen.

Artículo 79. *Supresión de la identificación de la línea conectada.*

Cuando los operadores citados en el apartado 1 del artículo 71 ofrezcan la facilidad de identificación de la línea conectada, el abonado que recibe la llamada deberá tener la posibilidad, mediante un procedimiento sencillo y gratuito, de suprimir la visualización al usuario que realiza la llamada de la identidad de la línea conectada.

Artículo 80. *Características técnicas.*

Los operadores citados en el apartado 1 del artículo 71 aplicarán, de manera general y siempre que sea factible, para la implantación de las facilidades de identificación de la línea de origen y de la línea conectada, las normas técnicas comunitarias que sean de aplicación. En su defecto, aplicarán las normas, especificaciones o recomendaciones de organismos europeos o, a falta de éstas, las adoptadas por organismos internacionales de normalización. En ausencia de todas las anteriores, se tendrán en cuenta las normas nacionales.

En cualquier caso, dichos operadores pondrán a disposición de los fabricantes de equipos terminales u otras entidades interesadas, de manera neutral, transparente y no discriminatoria, información actualizada sobre las características y normas técnicas aplicadas para la implantación en sus redes de las facilidades de identificación de la línea de origen y de la línea conectada. En lo que se refiere a la información que debe suministrarse a los fabricantes de equipos terminales, ésta deberá contener un nivel de detalle suficiente que permita el diseño de equipos capaces de hacer uso de todas las funcionalidades que forman parte de las facilidades de identificación de la línea de origen y de la línea conectada.

Artículo 81. *Responsabilidad de los operadores que tengan sus redes interconectadas.*

1. En el caso de que las redes de varios operadores estén interconectadas, será responsabilidad del operador desde cuya red se origine la llamada la generación y entrega en el punto de interconexión de la identidad de la línea de origen y el respeto de la posible marca de supresión que haya sido introducida por el usuario.

El operador cuya red sea el destino final de la llamada y preste la facilidad de identificación de la línea de origen deberá hacerlo atendiendo a la información recibida asociada a la llamada y en el marco de lo que se establece en los artículos anteriores.

2. Igualmente, en la prestación de la facilidad de identificación de la línea conectada, los operadores de las redes origen o destino de las llamadas serán responsables de la correcta provisión de las funcionalidades específicas que correspondan a su red.

El operador cuya red realice exclusivamente servicios de tránsito de las llamadas deberá transmitir en cada caso y de manera transparente la identidad de la línea de origen o de la línea conectada y sus marcas asociadas.

3. El envío de la información sobre la identidad de la línea de origen en la interconexión internacional con terceros países sólo se realizará hacia aquellos cuya normativa garantice el adecuado tratamiento de los datos de carácter personal. La relación de países a los que puede ser enviada información sobre la identidad de la línea de origen se establecerá por el Director de la Agencia Española de Protección de Datos, previo informe de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

Artículo 82. *Desvío automático de llamadas.*

Los operadores a los que se refiere el apartado 1 del artículo 71 deberán ofrecer a todos los abonados, por un procedimiento sencillo y gratuito, la posibilidad de evitar el desvío automático de llamadas a su terminal por parte de un tercero.

CAPÍTULO II

La interceptación legal de las comunicaciones

Sección 1.ª Disposiciones generales

Artículo 83. *Objeto.*

Es objeto de este capítulo el establecimiento del procedimiento que debe seguirse y las medidas que deberán adoptar, de conformidad con el artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones electrónicas.

Las únicas interceptaciones que estarán obligados a realizar los sujetos a los que se refiere el artículo 85 son las dispuestas en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, y en otras normas con rango de ley orgánica.

Artículo 84. *Definiciones.*

A los efectos de lo dispuesto en este capítulo, los términos definidos en este artículo tendrán el significado siguiente:

a) Interceptación legal: medida establecida por ley y adoptada por una autoridad judicial que acuerda o autoriza el acceso o la transmisión de las comunicaciones electrónicas de una persona, y la información relativa a la interceptación, a los agentes facultados, sin perjuicio de lo establecido en el artículo 579.4 de la Ley de Enjuiciamiento Criminal.

b) Interfaz de interceptación: localización física o lógica dentro de las instalaciones de los sujetos obligados en la que se proporcionan las comunicaciones electrónicas interceptadas y la información relativa a la interceptación a los agentes facultados. La interfaz de interceptación no es necesariamente un único punto fijo.

c) Orden de interceptación legal: resolución acordada por una autoridad judicial por la que se acuerda o autoriza la adopción de una medida de interceptación legal o se ordena lo necesario para su ejecución técnica a los sujetos obligados o un agente facultado.

d) Sujeto a la interceptación: la persona o las personas designadas, o bien incluidas de forma individualizadas, en la orden de interceptación legal cuyas comunicaciones electrónicas son objeto de la medida.

e) Agente facultado: policía judicial o personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar una interceptación legal.

f) Autoridad judicial: autoridad a la que la ley faculta para acordar o autorizar la adopción y ordenar la ejecución técnica de una medida de interceptación legal.

g) Centro de recepción de las interceptaciones: instalación de los agentes facultados que recibe las comunicaciones electrónicas interceptadas y la información relativa a la interceptación de un determinado sujeto sometido a interceptación.

h) Itinerancia: situación en la que se presta un servicio de comunicaciones electrónicas por una red distinta de la local en la que está inscrito el usuario.

i) Identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

Artículo 85. *Sujetos obligados y obligación de colaborar.*

1. Estarán obligados a seguir los procedimientos y adoptar las medidas a las que se refiere el artículo 83 los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones en España, con independencia de la naturaleza, ámbito territorial y momento en que tuvo efecto su habilitación.

Los operadores a los que se refiere el párrafo anterior estarán obligados a cumplir lo establecido en este capítulo, aun en el caso de que sólo presten en España acceso a una red pública de comunicaciones electrónicas, y todo aquel equipamiento susceptible de emplearse para realizar la interceptación se encuentre bajo la jurisdicción de otro Estado.

2. Cualquier operador de red que ponga ésta a disposición de un proveedor de servicios de comunicaciones electrónicas deberá colaborar con él en el cumplimiento de los requisitos de este capítulo.

Asimismo, cualquier otro proveedor de servicios de comunicaciones electrónicas disponibles al público que acuerde facilitar servicio de itinerancia con un proveedor principal estará obligado a colaborar con éste en el cumplimiento de los requisitos de este capítulo.

Artículo 86. *Requisitos generales.*

1. Los sujetos obligados deberán tener sus equipos configurados de forma que puedan facilitar el acceso de los agentes facultados a todas las comunicaciones transmitidas, generadas para su transmisión o recibidas por el sujeto de una interceptación legal y los datos de tráfico asociados a dicha comunicación. Junto con las comunicaciones deberán poder facilitar la información relativa a la interceptación que se enumera en el artículo 88, aun cuando la comunicación quede en mero intento por no llegar a establecerse. La correspondencia entre una comunicación y la información relativa a dicha interceptación se hará de tal manera que se pueda establecer entre ambos una correlación inequívoca, siempre que sea técnicamente posible.

2. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

3. Los sujetos obligados a los que hacen referencia los apartados anteriores deberán disponer de los medios técnicos y humanos que permitan el cumplimiento de las obligaciones establecidas en este reglamento.

Artículo 87. *Acceso a las comunicaciones electrónicas.*

1. El acceso a una comunicación electrónica por el sujeto obligado se hará excluyendo cualquier otra comunicación que no se incluya en el ámbito de aplicación de la orden de interceptación legal.

2. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímil.

3. El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

4. El acceso a las comunicaciones se facilitará aun cuando el sujeto de la interceptación utilice procedimientos para desviar las llamadas a otros servicios de comunicaciones electrónicas o a otros puntos de terminación de red, o a otros terminales, y aun cuando las llamadas sean procesadas por proveedores de servicios de comunicaciones electrónicas distintos de aquel al que se dirige la orden de interceptación, siempre que se pueda discernir la comunicación que es objeto de la orden de interceptación.

Artículo 88. *Información relativa a la interceptación.*

1. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades -en la acepción definida en el artículo 84.i)- del sujeto objeto de la medida de la interceptación.

b) Identidad o identidades -en la acepción definida en el artículo 84.i)- de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

2. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

3. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

Sección 2.ª Requisitos operacionales

Artículo 89. *Información previa a la interceptación.*

1. En el marco de la investigación legal a requerimiento de la autoridad judicial o cuando así lo determine una norma con rango legal, los sujetos obligados conforme al artículo 85 pondrán a disposición de la autoridad que lleve a cabo dicha investigación, con carácter

previo a la interceptación legal, información actualizada relativa a los datos a que hace referencia el artículo 90.

2. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

3. Los sujetos obligados conforme al artículo 85 deben tener dispuesta la organización necesaria que garantice el cumplimiento de la orden de interceptación legal en los términos establecidos en el artículo 99. Para ello, deberán identificar la unidad habilitada para recibir una orden de interceptación que les sea notificada y establecer los procedimientos internos para dar soporte a las actuaciones necesarias.

Artículo 90. *Información para la interceptación.*

La interceptación se llevará a efecto si en la orden de interceptación legal se incluye, al menos, uno de los datos siguientes:

a) La identificación del abonado o usuario sujeto a la interceptación.

b) La ubicación donde se encuentre un punto de terminación de red al que el operador da servicio.

c) Un identificador de punto de terminación de red (dirección), o de terminal, al que el proveedor de servicios de comunicaciones electrónicas da servicio.

d) El código de identificación en caso de que sea el usuario el que active el terminal para la comunicación.

e) Cualquier otra identidad -en la acepción definida en el artículo 84.i)- que corresponda al sujeto especificado en la orden de interceptación legal.

Artículo 91. *Lugares para la interceptación.*

Para delimitar las responsabilidades y asegurar mejor el secreto de las telecomunicaciones frente a terceras partes ajenas, su interceptación se realizará preferentemente en salas con acceso restringido que garantice la confidencialidad en los términos del artículo 92. En cualquier caso, se deberá garantizar el secreto de las comunicaciones, para lo que deberán adoptarse las medidas técnicas necesarias.

Artículo 92. *Personal autorizado.*

Sin perjuicio de lo establecido en la legislación sobre protección de materias clasificadas, el sujeto obligado será responsable de que sólo el personal que haya sido expresamente autorizado pueda acceder a los mecanismos de interceptación.

Artículo 93. *Confidencialidad.*

1. Todo documento relativo a las operaciones de interceptación, al igual que cualquier información relativa a procedimientos de interceptación, será de circulación restringida a las personas autorizadas de acuerdo con lo establecido en el artículo anterior y sin perjuicio de lo establecido en la legislación sobre materias clasificadas.

2. La interceptación se efectuará de manera que ni el sujeto a la interceptación, ni ninguna persona no autorizada, pueda tener conocimiento de ella. En particular, las prestaciones del servicio deben ser las mismas que en ausencia de interceptación, y ninguna alteración de éste puede permitir sospechar que se está realizando una interceptación.

Artículo 94. *Acceso en tiempo real.*

La interceptación se realizará en tiempo real, sin más retardo que el mínimo imprescindible para realizar el encaminamiento y transmisión, e ininterrumpidamente durante el plazo establecido en la orden de interceptación legal. Si no se pudiera facilitar la

información relativa a la interceptación a la que se refiere el artículo 88 en tiempo real por causa de fuerza mayor, se efectuará al finalizar la conexión y, en todo caso, lo antes posible.

Artículo 95. *Interfaces de interceptación.*

Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

Artículo 96. *Señal en claro y calidad de la señal entregada.*

En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

Artículo 97. *Secreto de las comunicaciones.*

Las comunicaciones y la información relativa a la interceptación sólo se facilitarán al agente facultado. Para ello, los sujetos a los que se refiere el artículo 85 pondrán todos los medios necesarios para impedir la manipulación de los mecanismos de interceptación, y para garantizar la autenticidad, confidencialidad e integridad de la información obtenida con la interceptación.

Artículo 98. *Interceptaciones múltiples y simultáneas.*

1. Los sujetos obligados garantizarán que pueda llevarse a cabo de forma múltiple más de una interceptación legal en relación con una línea, un usuario o abonado.

2. El número máximo de interceptaciones simultáneas que ha de ser capaz de proveer un operador de red o proveedor de servicio se establecerá mediante orden ministerial.

Artículo 99. *Plazo de ejecución de la interceptación.*

1. El plazo de ejecución de una orden de interceptación legal será el fijado en ella. Cuando no se establezca plazo, las órdenes se ejecutarán antes de las 12:00 horas del día laborable siguiente al que el sujeto obligado reciba la orden de interceptación legal.

2. Cuando la orden de interceptación legal establezca la urgencia de su ejecución, los sujetos obligados deberán ejecutarla con la mayor brevedad posible teniendo en cuenta lo dispuesto en la orden de interceptación.

3. La activación del mecanismo de interceptación será notificada al agente facultado por el medio que se acuerde entre dicho agente y el sujeto obligado.

Artículo 100. *Abono del coste de la interceptación.*

El operador o proveedor de servicios de comunicaciones electrónicas que haya realizado una interceptación legal tendrá derecho a que se le abonen las cantidades en que haya incurrido por el uso de canales de comunicación, temporales o permanentes, que establezca de modo específico para facilitar la transmisión de las comunicaciones electrónicas interceptadas y la información relativa a la interceptación a los agentes facultados, teniendo en cuenta los precios que se apliquen en cada caso. En ningún caso serán objeto de compensación los gastos relativos a equipamientos específicos para la interceptación de que, en su caso, tuviera que dotarse, toda vez que constituyen una carga accesoria a los deberes de la habilitación correspondiente.

Artículo 101. *Infracciones.*

1. Sin perjuicio de la responsabilidad penal en que pueda incurrirse en la ejecución de las interceptaciones, el incumplimiento de las órdenes de interceptación legal será constitutivo de una infracción sancionable de acuerdo con las previsiones del título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. En la imposición de la sanción se valorará el retraso en la ejecución de la interceptación y otros perjuicios causados por el incumplimiento.

TÍTULO VI

Derechos de los consumidores que sean personas físicas y otros usuarios finales

CAPÍTULO I

Disposiciones generales

Artículos 102 a 104.

(Derogados)

CAPÍTULO II

Contratos

Artículos 105 a 108.

(Derogados)

CAPÍTULO III

Derechos y obligaciones de transparencia, información y calidad

Artículos 109 a 111.

(Derogados)

CAPÍTULO IV

Derechos en relación con el servicio telefónico disponible al público

Artículos 112 a 119.

(Derogados)

CAPÍTULO V

Derechos en relación con el servicio de acceso a Internet

Artículo 120. *Derecho a compensación por la interrupción temporal del servicio de acceso a Internet.*

(Derogado)

Disposición adicional única. *Cálculo del coste neto del servicio universal en caso de recepción de ayudas.*

Los operadores designados para la prestación del servicio universal podrán beneficiarse de ayudas procedentes de los regímenes en vigor en los términos establecidos en su normativa específica y, en particular, de las procedentes de los fondos estructurales de la Unión Europea. En estos supuestos, la Comisión del Mercado de las Telecomunicaciones

evaluará el coste neto de prestación del servicio universal a los efectos y con las particularidades que se establezcan en la concesión de dichas ayudas.

Disposición transitoria primera. *Títulos habilitantes para la prestación de servicios y el establecimiento de redes de comunicaciones electrónicas anteriores a este reglamento.*

1. La Comisión del Mercado de las Telecomunicaciones inscribirá en el Registro de operadores regulado en este reglamento a los que tengan títulos habilitantes anteriores a la entrada en vigor de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. A estos efectos, en el Registro de operadores se inscribirá a todos los titulares de autorizaciones generales, licencias individuales y autorizaciones provisionales otorgadas o transformadas conforme a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, e inscritos en los correspondientes registros especiales de titulares de licencias individuales y autorizaciones generales.

2. La Comisión del Mercado de las Telecomunicaciones inscribirá en el Registro de operadores regulado en este reglamento a los operadores que hayan obtenido su habilitación tras la entrada en vigor de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y antes de la entrada en vigor de este real decreto, y que, conforme a la disposición transitoria primera de dicha ley, estén inscritos en el Registro especial de titulares de autorizaciones generales.

3. El plazo de tres años tras el cual los operadores deben comunicar a la Comisión del Mercado de las Telecomunicaciones su intención de continuar prestando el servicio conforme a lo establecido en el artículo 5.2 de este reglamento comenzará a contar, para los operadores que hayan obtenido su habilitación con anterioridad a éste, en el momento de su entrada en vigor.

Disposición transitoria segunda. *Régimen transitorio aplicable al servicio universal.*

(Derogada)

Disposición transitoria tercera. *Vigencia de la Orden CTE/711/2002, de 26 de marzo, del Real Decreto 903/1997, de 16 de junio, y de la Orden de 14 de octubre de 1999.*

Hasta que se apruebe la orden prevista en el artículo 112, continuará siendo de aplicación la Orden CTE/711/2002, de 26 de marzo.

Asimismo, conservan su vigencia, en todo lo que no se oponga a este reglamento, el Real Decreto 903/1997, de 16 de junio, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112, y la Orden de 14 de octubre de 1999, sobre condiciones de suministro de información relevante para la prestación del servicio de llamadas de urgencia a través del número 112.

Disposición transitoria cuarta. *Prestación de los servicios a los que se refiere la disposición transitoria cuarta de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

Mientras sea de aplicación lo dispuesto en la disposición transitoria cuarta de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, no obstante lo dispuesto en el artículo 53, las características técnicas de prestación de los servicios a que se refiere dicho artículo, sus condiciones de prestación y de financiación se fijarán por real decreto.

Mientras sea de aplicación lo dispuesto en la disposición transitoria cuarta de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, no obstante lo dispuesto en el artículo 54, las características técnicas de prestación de los servicios a que se refiere dicho artículo, sus condiciones de prestación y de financiación se fijarán por orden del Ministro de la Presidencia, a propuesta de los Ministros de Industria, Turismo y Comercio y de Fomento.

Asimismo, hasta que se aprueben las disposiciones a que se refieren los párrafos anteriores, a dichos servicios les serán de aplicación las condiciones de prestación que actualmente se encuentran establecidas.

Disposición transitoria quinta. *Obligaciones de servicio público del servicio portador de televisión analógica.*

Continuarán en vigor las obligaciones de servicio público y la garantía de continuidad en la prestación de los servicios portadores soporte de los de difusión televisiva establecidos en el Real Decreto Ley 16/1999, de 15 de octubre, en los términos desarrollados en el vigente Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico, para los servicios de televisión analógica, hasta tanto se den los supuestos previsto en el artículo 2 del Plan técnico nacional de televisión digital terrenal, aprobado por el Real Decreto 2169/1998, de 9 de octubre.

Disposición transitoria sexta. *Plazo para el cumplimiento de los requisitos en materia de interceptación legal de las comunicaciones.*

Los operadores habilitados para la prestación de servicios de comunicaciones electrónicas disponibles al público o la explotación de redes públicas de comunicaciones electrónicas y que se encuentren obligados al cumplimiento de lo previsto en el capítulo II del título V de este reglamento, de acuerdo con su artículo 85, deberán cumplir las obligaciones establecidas en él en el plazo de un año desde su entrada en vigor.

No obstante lo dispuesto en el párrafo anterior, las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones entrarán en vigor en el plazo que en su caso establezca la orden ministerial correspondiente. Dicha orden se aprobará previo informe de una comisión en la que se integrarán representantes de los ministerios afectados y de los operadores. Conforme al principio de proporcionalidad establecido en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, y la normativa comunitaria, en su aprobación se tomará en consideración la proporción entre los objetivos a conseguir y los costes en que se incurra.

Disposición transitoria séptima. *Guías de servicios de comunicaciones electrónicas.*

Para la inclusión en las guías de los datos de los abonados que, a la entrada en vigor de este reglamento, ya figuren en la guía prevista en el artículo 30, bastará con que, en el plazo de un mes tras la recepción de la comunicación a que se refiere el artículo 67.1, el abonado no se oponga expresamente a dicha inclusión.

Disposición transitoria octava. *Derechos de los consumidores y usuarios.*

Hasta tanto no se desarrolle mediante orden ministerial el título VI de este reglamento en materia de derechos de los consumidores y usuarios y servicios de tarifas superiores, seguirá siendo de aplicación, en cuanto no se oponga a este reglamento, la Orden PRE/361/2002, de 14 de febrero, de desarrollo, en lo relativo a los derechos de los usuarios y a los servicios de tarificación adicional, del título IV del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones. En aquella orden se establecerá el régimen aplicable a los servicios de mensajería que se prestan a través de números cortos.

Disposición transitoria novena. *Disposiciones relativas a la prestación de las facilidades de identificación de la línea de origen o de la línea conectada.*

1. Los operadores que, en el momento de entrada en vigor de este reglamento, se encuentren prestando las facilidades de identificación de la línea de origen y de la línea conectada, deberán cumplir lo previsto en el segundo párrafo del apartado 2 del artículo 71 y en el último párrafo de dicho artículo en el plazo de un mes desde dicha entrada en vigor.

2. Hasta que se apruebe la resolución que atribuya un número corto como código para la supresión en origen por el usuario, llamada a llamada, de la identificación de la línea de origen, continuará vigente el código establecido en la Resolución de la Secretaría General de Comunicaciones, de 2 de diciembre de 1998, por la que se atribuye el código 067 al servicio de supresión en origen llamada a llamada de la identificación de la línea llamante, con las

modificaciones que, en su caso, se establezcan por las disposiciones de desarrollo del plan de numeración.

Disposición final única. *Modelo de declaración normalizada.*

En el plazo de un mes desde la entrada en vigor de este reglamento, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información aprobará, a propuesta del Consejo de la Comisión del Mercado de las Telecomunicaciones, el modelo de declaración normalizada de notificación e inscripción al que se refiere el artículo 11.

§ 46

Ley 58/2003, de 17 de diciembre, General Tributaria. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 302, de 18 de diciembre de 2003
Última modificación: 10 de julio de 2021
Referencia: BOE-A-2003-23186

[. . .]

TÍTULO III

La aplicación de los tributos

CAPÍTULO I

Principios generales

[. . .]

Sección 3.ª Colaboración social en la aplicación de los tributos

[. . .]

Artículo 93. *Obligaciones de información.*

1. Las personas físicas o jurídicas, públicas o privadas, así como las entidades mencionadas en el apartado 4 del artículo 35 de esta ley, estarán obligadas a proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes con trascendencia tributaria relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas.

En particular:

a) Los retenedores y los obligados a realizar ingresos a cuenta deberán presentar relaciones de los pagos dinerarios o en especie realizados a otras personas o entidades.

b) Las sociedades, asociaciones, colegios profesionales u otras entidades que, entre sus funciones, realicen la de cobro de honorarios profesionales o de derechos derivados de la propiedad intelectual, industrial, de autor u otros por cuenta de sus socios, asociados o colegiados, deberán comunicar estos datos a la Administración tributaria.

A la misma obligación quedarán sujetas aquellas personas o entidades, incluidas las bancarias, crediticias o de mediación financiera en general que, legal, estatutaria o habitualmente, realicen la gestión o intervención en el cobro de honorarios profesionales o

en el de comisiones, por las actividades de captación, colocación, cesión o mediación en el mercado de capitales.

c) Las personas o entidades depositarias de dinero en efectivo o en cuentas, valores u otros bienes de deudores a la Administración tributaria en período ejecutivo estarán obligadas a informar a los órganos de recaudación y a cumplir los requerimientos efectuados por los mismos en el ejercicio de sus funciones.

d) Las personas y entidades que, por aplicación de la normativa vigente, conocieran o estuvieran en disposición de conocer la identificación de los beneficiarios últimos de las acciones deberán cumplir ante la Administración tributaria con los requerimientos u obligaciones de información que reglamentariamente se establezcan respecto a dicha identificación.

2. Las obligaciones a las que se refiere el apartado anterior deberán cumplirse con carácter general en la forma y plazos que reglamentariamente se determinen, o mediante requerimiento individualizado de la Administración tributaria que podrá efectuarse en cualquier momento posterior a la realización de las operaciones relacionadas con los datos o antecedentes requeridos.

3. El incumplimiento de las obligaciones establecidas en este artículo no podrá ampararse en el secreto bancario.

Los requerimientos individualizados relativos a los movimientos de cuentas corrientes, depósitos de ahorro y a plazo, cuentas de préstamos y créditos y demás operaciones activas y pasivas, incluidas las que se reflejen en cuentas transitorias o se materialicen en la emisión de cheques u otras órdenes de pago, de los bancos, cajas de ahorro, cooperativas de crédito y cuantas entidades se dediquen al tráfico bancario o crediticio, podrán efectuarse en el ejercicio de las funciones de inspección o recaudación, previa autorización del órgano de la Administración tributaria que reglamentariamente se determine.

Los requerimientos individualizados deberán precisar los datos identificativos del cheque u orden de pago de que se trate, o bien las operaciones objeto de investigación, los obligados tributarios afectados, titulares o autorizados, y el período de tiempo al que se refieren.

La investigación realizada según lo dispuesto en este apartado podrá afectar al origen y destino de los movimientos o de los cheques u otras órdenes de pago, si bien en estos casos no podrá exceder de la identificación de las personas y de las cuentas en las que se encuentre dicho origen y destino.

4. Los funcionarios públicos, incluidos los profesionales oficiales, estarán obligados a colaborar con la Administración tributaria suministrando toda clase de información con trascendencia tributaria de la que dispongan, salvo que sea aplicable:

a) El secreto del contenido de la correspondencia.

b) El secreto de los datos que se hayan suministrado a la Administración para una finalidad exclusivamente estadística.

c) El secreto del protocolo notarial, que abarcará los instrumentos públicos a los que se refieren los artículos 34 y 35 de la Ley de 28 de mayo de 1862, del Notariado, y los relativos a cuestiones matrimoniales, con excepción de los referentes al régimen económico de la sociedad conyugal.

5. La obligación de los demás profesionales de facilitar información con trascendencia tributaria a la Administración tributaria no alcanzará a los datos privados no patrimoniales que conozcan por razón del ejercicio de su actividad cuya revelación atente contra el honor o la intimidad personal y familiar. Tampoco alcanzará a aquellos datos confidenciales de sus clientes de los que tengan conocimiento como consecuencia de la prestación de servicios profesionales de asesoramiento o defensa.

Los profesionales no podrán invocar el secreto profesional para impedir la comprobación de su propia situación tributaria.

Artículo 94. *Autoridades sometidas al deber de informar y colaborar.*

1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y

asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones.

Asimismo, participarán en la gestión o exacción de los tributos mediante las advertencias, repercusiones y retenciones, documentales o pecuniarias, de acuerdo con lo previsto en las leyes o disposiciones reglamentarias vigentes.

2. A las mismas obligaciones quedarán sujetos los partidos políticos, sindicatos y asociaciones empresariales.

3. Los juzgados y tribunales deberán facilitar a la Administración tributaria, de oficio o a requerimiento de la misma, cuantos datos con trascendencia tributaria se desprendan de las actuaciones judiciales de las que conozcan, respetando, en su caso, el secreto de las diligencias sumariales.

4. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo, así como la Secretaría de ambas comisiones, facilitarán a la Administración tributaria cuantos datos con trascendencia tributaria obtengan en el ejercicio de sus funciones, de oficio, con carácter general o mediante requerimiento individualizado en los términos que reglamentariamente se establezcan.

Los órganos de la Administración tributaria podrán utilizar la información suministrada para la regularización de la situación tributaria de los obligados en el curso del procedimiento de comprobación o de inspección, sin que sea necesario efectuar el requerimiento al que se refiere el apartado 3 del artículo anterior.

5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 95. *Carácter reservado de los datos con trascendencia tributaria.*

1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:

a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada.

b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.

c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social y contra el fraude en la obtención y disfrute de las prestaciones a cargo del sistema; así como para la determinación del nivel de aportación de cada usuario en las prestaciones del Sistema Nacional de Salud.

d) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea.

e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.

f) La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Fiscal.

g) La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de Administración Tributaria.

h) La colaboración con los jueces y tribunales para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa en la que, previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.

i) La colaboración con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y con la Secretaría de ambas comisiones, en el ejercicio de sus funciones respectivas.

j) La colaboración con órganos o entidades de derecho público encargados de la recaudación de recursos públicos no tributarios para la correcta identificación de los obligados al pago y con la Dirección General de Tráfico para la práctica de las notificaciones a los mismos, dirigidas al cobro de tales recursos.

k) La colaboración con las Administraciones públicas para el desarrollo de sus funciones, previa autorización de los obligados tributarios a que se refieran los datos suministrados.

l) La colaboración con la Intervención General de la Administración del Estado en el ejercicio de sus funciones de control de la gestión económico-financiera, el seguimiento del déficit público, el control de subvenciones y ayudas públicas y la lucha contra la morosidad en las operaciones comerciales de las entidades del Sector Público.

m) La colaboración con la Oficina de Recuperación y Gestión de Activos mediante la cesión de los datos, informes o antecedentes necesarios para la localización de los bienes embargados o decomisados en un proceso penal, previa acreditación de esta circunstancia.

2. En los casos de cesión previstos en el apartado anterior, la información de carácter tributario deberá ser suministrada preferentemente mediante la utilización de medios informáticos o telemáticos. Cuando las Administraciones públicas puedan disponer de la información por dichos medios, no podrán exigir a los interesados la aportación de certificados de la Administración tributaria en relación con dicha información.

3. La Administración tributaria adoptará las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado.

Cuantas autoridades o funcionarios tengan conocimiento de estos datos, informes o antecedentes estarán obligados al más estricto y completo sigilo respecto de ellos, salvo en los casos citados. Con independencia de las responsabilidades penales o civiles que pudieran derivarse, la infracción de este particular deber de sigilo se considerará siempre falta disciplinaria muy grave.

Cuando se aprecie la posible existencia de un delito no perseguible únicamente a instancia de persona agraviada, la Administración tributaria deducirá el tanto de culpa o remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito. También podrá iniciarse directamente el oportuno procedimiento mediante querella a través del Servicio Jurídico competente.

4. El carácter reservado de los datos establecido en este artículo no impedirá la publicidad de los mismos cuando ésta se derive de la normativa de la Unión Europea.

5. Los retenedores y obligados a realizar ingresos a cuenta sólo podrán utilizar los datos, informes o antecedentes relativos a otros obligados tributarios para el correcto cumplimiento y efectiva aplicación de la obligación de realizar pagos a cuenta. Dichos datos deberán ser comunicados a la Administración tributaria en los casos previstos en la normativa propia de cada tributo.

Salvo lo dispuesto en el párrafo anterior, los referidos datos, informes o antecedentes tienen carácter reservado. Los retenedores y obligados a realizar ingresos a cuenta quedan sujetos al más estricto y completo sigilo respecto de ellos.

6. La cesión de información en el ámbito de la asistencia mutua se regirá por lo dispuesto en el artículo 177 ter de esta Ley.

Artículo 95 bis. *Publicidad de situaciones de incumplimiento relevante de las obligaciones tributarias.*

1. La Administración Tributaria acordará la publicación periódica de listados comprensivos de deudores a la Hacienda Pública, incluidos los que tengan la condición de deudores al haber sido declarados responsables solidarios, por deudas o sanciones tributarias cuando concurran las siguientes circunstancias:

a) Que el importe total de las deudas y sanciones tributarias pendientes de ingreso, incluidas en su caso las que se hubieran exigido tras la declaración de responsabilidad solidaria, supere el importe de 600.000 euros.

b) Que dichas deudas o sanciones tributarias no hubiesen sido pagadas transcurrido el plazo original de ingreso en periodo voluntario.

En el supuesto de deudas incluidas en acuerdos de declaración de responsabilidad será necesario que haya transcurrido el plazo de pago del artículo 62.2 de esta Ley tras la notificación del acuerdo de declaración de responsabilidad y, en su caso, del acuerdo de exigencia de pago.

A efectos de lo dispuesto en este artículo no se incluirán aquellas deudas y sanciones tributarias que se encuentren aplazadas o suspendidas.

2. En dichos listados se incluirá la siguiente información:

a) La identificación de los deudores conforme al siguiente detalle:

– Personas Físicas: nombre apellidos y NIF.

– Personas Jurídicas y entidades del artículo 35.4 de esta Ley: razón o denominación social completa y NIF.

b) El importe conjunto de las deudas y sanciones pendientes de pago tenidas en cuenta a efectos de la publicación.

3. En el ámbito del Estado, la publicidad regulada en este artículo se referirá exclusivamente a los tributos de titularidad estatal para los que la aplicación de los tributos, el ejercicio de la potestad sancionadora y las facultades de revisión estén atribuidas en exclusiva a los órganos de la Administración Tributaria del Estado no habiendo existido delegación alguna de competencias en estos ámbitos a favor de las Comunidades Autónomas o Entes Locales.

La publicidad regulada en este artículo resultará de aplicación respecto a los tributos que integran la deuda aduanera.

4. La determinación de la concurrencia de los requisitos exigidos para la inclusión en el listado tomará como fecha de referencia el 31 de diciembre del año anterior al del acuerdo de publicación, cualquiera que sea la cantidad pendiente de ingreso a la fecha de dicho acuerdo.

La propuesta de inclusión en el listado será comunicada al deudor afectado, que podrá formular alegaciones en el plazo de 10 días contados a partir del siguiente al de recepción de la comunicación. A estos efectos será suficiente para entender realizada dicha comunicación la acreditación por parte de la Administración Tributaria de haber realizado un intento de notificación de la misma que contenga el texto íntegro de su contenido en el domicilio fiscal del interesado.

En el caso de que los deudores paguen la totalidad de la cantidad adeudada a la fecha de referencia antes de la finalización del plazo para formular alegaciones, no se incluirán en los listados comprensivos de deudores a la Hacienda Pública por deudas o sanciones tributarias.

Las alegaciones habrán de referirse exclusivamente a la existencia de errores materiales, de hecho o aritméticos en relación con los requisitos señalados en el apartado 1 o a los pagos efectuados por el deudor a que se refiere el párrafo anterior, debiéndose aportar en este caso justificación fehaciente de dichos pagos.

Como consecuencia del trámite de alegaciones, la Administración podrá acordar la rectificación del listado cuando se acredite fehacientemente que no concurren los requisitos legales determinados en el apartado 1 o cuando a la conclusión del plazo para formular alegaciones se hubiera satisfecho la totalidad de las deudas o sanciones tributarias.

Dicha rectificación también podrá ser acordada de oficio.

Practicadas las rectificaciones oportunas, se dictará el acuerdo de publicación.

La notificación del acuerdo se entenderá producida con su publicación y la del listado.

Mediante Orden Ministerial se establecerán la fecha de publicación, que deberá producirse en todo caso durante el primer semestre de cada año, y los correspondientes ficheros y registros.

La publicación se efectuará en todo caso por medios electrónicos, debiendo adoptarse las medidas necesarias para impedir la indexación de su contenido a través de motores de búsqueda en Internet y los listados dejarán de ser accesibles una vez transcurridos tres meses desde la fecha de publicación.

El tratamiento de datos necesarios para la publicación se sujetará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como por su normativa de desarrollo.

5. En el ámbito de competencias del Estado, será competente para dictar los acuerdos de publicación regulados en este artículo el Director General de la Agencia Estatal de Administración Tributaria.

6. En la publicación del listado se especificará que la situación en el mismo reflejada es la existente a la fecha de referencia señalada en el apartado 4, sin que la publicación del listado resulte afectada por las actuaciones realizadas por el deudor con posterioridad a dicha fecha de referencia, salvo que se verifique el pago en los casos y con los requisitos señalados en dicho apartado.

Lo dispuesto en este artículo no afectará en modo alguno al régimen de impugnación establecido en esta Ley en relación con las actuaciones y procedimientos de los que se deriven las deudas y sanciones tributarias ni tampoco a las actuaciones y procedimientos de aplicación de los tributos iniciados o que se pudieran iniciar con posterioridad en relación con las mismas.

Las actuaciones desarrolladas en el procedimiento establecido en este artículo en orden a la publicación de la información en el mismo regulada no constituyen causa de interrupción a los efectos previstos en el artículo 68 de esta Ley.

7. El acuerdo de publicación del listado pondrá fin a la vía administrativa.

Sección 4.ª Tecnologías informáticas y telemáticas

Artículo 96. *Utilización de tecnologías informáticas y telemáticas.*

1. La Administración tributaria promoverá la utilización de las técnicas y medios electrónicos, informáticos y telemáticos necesarios para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que la Constitución y las leyes establezcan.

2. Cuando sea compatible con los medios técnicos de que disponga la Administración tributaria, los ciudadanos podrán relacionarse con ella para ejercer sus derechos y cumplir con sus obligaciones a través de técnicas y medios electrónicos, informáticos o telemáticos con las garantías y requisitos previstos en cada procedimiento.

3. Los procedimientos y actuaciones en los que se utilicen técnicas y medios electrónicos, informáticos y telemáticos garantizarán la identificación de la Administración tributaria actuante y el ejercicio de su competencia. Además, cuando la Administración tributaria actúe de forma automatizada se garantizará la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los recursos que puedan interponerse.

4. Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por la Administración tributaria para el ejercicio de sus potestades habrán de ser previamente aprobados por ésta en la forma que se determine reglamentariamente.

5. Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por la Administración tributaria, o los que ésta emita como copias

de originales almacenados por estos mismos medios, así como las imágenes electrónicas de los documentos originales o sus copias, tendrán la misma validez y eficacia que los documentos originales, siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por la normativa aplicable.

CAPÍTULO II

Normas comunes sobre actuaciones y procedimientos tributarios

[. . .]

Sección 1.ª Especialidades de los procedimientos administrativos en materia tributaria

Subsección 1.ª Fases de los procedimientos tributarios

[. . .]

Artículo 99. *Desarrollo de las actuaciones y procedimientos tributarios.*

1. En el desarrollo de las actuaciones y procedimientos tributarios, la Administración facilitará en todo momento a los obligados tributarios el ejercicio de los derechos y el cumplimiento de sus obligaciones, en los términos previstos en los apartados siguientes.

2. Los obligados tributarios pueden rehusar la presentación de los documentos que no resulten exigibles por la normativa tributaria y de aquellos que hayan sido previamente presentados por ellos mismos y que se encuentren en poder de la Administración tributaria actuante. Se podrá, en todo caso, requerir al interesado la ratificación de datos específicos propios o de terceros, previamente aportados.

3. Los obligados tributarios tienen derecho a que se les expida certificación de las autoliquidaciones, declaraciones y comunicaciones que hayan presentado o de extremos concretos contenidos en las mismas.

4. El obligado que sea parte en una actuación o procedimiento tributario podrá obtener a su costa copia de los documentos que figuren en el expediente, salvo que afecten a intereses de terceros o a la intimidad de otras personas o que así lo disponga la normativa vigente. Las copias se facilitarán en el trámite de audiencia o, en defecto de éste, en el de alegaciones posterior a la propuesta de resolución.

5. El acceso a los registros y documentos que formen parte de un expediente concluido a la fecha de la solicitud y que obren en los archivos administrativos únicamente podrá ser solicitado por el obligado tributario que haya sido parte en el procedimiento tributario, sin perjuicio de lo dispuesto en el artículo 95 de esta ley.

6. Para la práctica de la prueba en los procedimientos tributarios no será necesaria la apertura de un período específico ni la comunicación previa de las actuaciones a los interesados.

7. Las actuaciones de la Administración tributaria en los procedimientos de aplicación de los tributos se documentarán en comunicaciones, diligencias, informes y otros documentos previstos en la normativa específica de cada procedimiento.

Las comunicaciones son los documentos a través de los cuales la Administración notifica al obligado tributario el inicio del procedimiento u otros hechos o circunstancias relativos al mismo o efectúa los requerimientos que sean necesarios a cualquier persona o entidad. Las comunicaciones podrán incorporarse al contenido de las diligencias que se extiendan.

Las diligencias son los documentos públicos que se extienden para hacer constar hechos, así como las manifestaciones del obligado tributario o persona con la que se entiendan las actuaciones. Las diligencias no podrán contener propuestas de liquidaciones tributarias.

Los órganos de la Administración tributaria emitirán, de oficio o a petición de terceros, los informes que sean preceptivos conforme al ordenamiento jurídico, los que soliciten otros órganos y servicios de las Administraciones públicas o los poderes legislativo y judicial, en

los términos previstos por las leyes, y los que resulten necesarios para la aplicación de los tributos.

8. En los procedimientos tributarios se podrá prescindir del trámite de audiencia previo a la propuesta de resolución cuando se suscriban actas con acuerdo o cuando en las normas reguladoras del procedimiento esté previsto un trámite de alegaciones posterior a dicha propuesta. En este último caso, el expediente se pondrá de manifiesto en el trámite de alegaciones.

El trámite de alegaciones no podrá tener una duración inferior a 10 días ni superior a 15.

9. Las actuaciones de la Administración y de los obligados tributarios en los procedimientos de aplicación de los tributos podrán realizarse a través de sistemas digitales que, mediante la videoconferencia u otro sistema similar, permitan la comunicación bidireccional y simultánea de imagen y sonido, la interacción visual, auditiva y verbal entre los obligados tributarios y el órgano actuante, y garanticen la transmisión y recepción seguras de los documentos que, en su caso, recojan el resultado de las actuaciones realizadas, asegurando su autoría, autenticidad e integridad.

La utilización de estos sistemas se producirá cuando lo determine la Administración Tributaria y requerirá la conformidad del obligado tributario en relación con su uso y con la fecha y hora de su desarrollo.

[. . .]

Sección 3.ª Notificaciones

[. . .]

Artículo 112. *Notificación por comparecencia.*

1. Cuando no sea posible efectuar la notificación al interesado o a su representante por causas no imputables a la Administración tributaria e intentada al menos dos veces en el domicilio fiscal, o en el designado por el interesado si se trata de un procedimiento iniciado a solicitud del mismo, se harán constar en el expediente las circunstancias de los intentos de notificación. Será suficiente un solo intento cuando el destinatario conste como desconocido en dicho domicilio o lugar.

En este supuesto se citará al interesado o a su representante para ser notificados por comparecencia por medio de anuncios que se publicarán, por una sola vez para cada interesado, en el "Boletín Oficial del Estado".

La publicación en el "Boletín Oficial del Estado" se efectuará los lunes, miércoles y viernes de cada semana. Estos anuncios podrán exponerse asimismo en la oficina de la Administración tributaria correspondiente al último domicilio fiscal conocido. En el caso de que el último domicilio conocido radicara en el extranjero, el anuncio se podrá exponer en el consulado o sección consular de la embajada correspondiente.

2. En la publicación constará la relación de notificaciones pendientes con indicación del obligado tributario o su representante, el procedimiento que las motiva, el órgano competente de su tramitación y el lugar y plazo en que el destinatario de las mismas deberá comparecer para ser notificado.

En todo caso, la comparecencia deberá producirse en el plazo de 15 días naturales, contados desde el siguiente al de la publicación del anuncio en el "Boletín Oficial del Estado". Transcurrido dicho plazo sin comparecer, la notificación se entenderá producida a todos los efectos legales el día siguiente al del vencimiento del plazo señalado.

3. Cuando el inicio de un procedimiento o cualquiera de sus trámites se entiendan notificados por no haber comparecido el obligado tributario o su representante, se le tendrá por notificado de las sucesivas actuaciones y diligencias de dicho procedimiento, y se mantendrá el derecho que le asiste a comparecer en cualquier momento del mismo. No obstante, las liquidaciones que se dicten en el procedimiento y los acuerdos de enajenación de los bienes embargados deberán ser notificados con arreglo a lo establecido en esta Sección.

[. . .]

§ 47

Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos. [Inclusión parcial]

Ministerio de Economía y Hacienda
«BOE» núm. 213, de 5 de septiembre de 2007
Última modificación: 16 de junio de 2021
Referencia: BOE-A-2007-15984

[. . .]

TÍTULO II

Las obligaciones tributarias formales

CAPÍTULO I

Las obligaciones censales

[. . .]

Artículo 2. *Censos de la Administración tributaria.*

1. Cada Administración tributaria podrá disponer de sus propios censos tributarios a efectos de la aplicación de sus tributos propios y cedidos.

2. Cualquier censo tributario incluirá necesariamente los siguientes datos:

a) Nombre y apellidos o razón social o denominación completa, así como el anagrama, si lo tuviera.

b) Numero de identificación fiscal.

c) Domicilio fiscal.

d) En su caso, domicilio en el extranjero.

3. Las Administraciones tributarias de las comunidades autónomas y ciudades con estatuto de autonomía comunicarán con periodicidad mensual a la Agencia Estatal de Administración Tributaria la información censal de que dispongan a efectos de consolidar esta.

La Agencia Estatal de Administración Tributaria comunicará con periodicidad mensual a las Administraciones tributarias de las comunidades autónomas y ciudades con estatuto de autonomía la variación de los datos a que se refiere el apartado anterior que se encuentren incluidos en el Censo de Obligados Tributarios regulado en el artículo 4.

4. La Agencia Estatal de Administración Tributaria podrá suscribir convenios de colaboración con las entidades locales para el intercambio de información censal.

5. Las personas o entidades incluidas en los censos tributarios tendrán derecho a conocer sus datos censales y podrán solicitar, a tal efecto, que se les expida el correspondiente certificado. Sin perjuicio de lo anterior, será aplicable a los referidos datos lo establecido en el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Los obligados tributarios tendrán derecho a la rectificación o cancelación de sus datos personales cuando resulten inexactos o incompletos de acuerdo con lo previsto en la legislación en materia de protección de datos de carácter personal.

[. . .]

Subsección 2.ª Las declaraciones censales en el ámbito de competencias del Estado

[. . .]

Artículo 10. *Declaración de modificación en el Censo de Empresarios, Profesionales y Retenedores.*

1. Cuando se modifique cualquiera de los datos recogidos en la declaración de alta o en cualquier otra declaración de modificación posterior, el obligado tributario deberá comunicar a la Administración tributaria, mediante la correspondiente declaración, dicha modificación.

2. Esta declaración, en particular, servirá para:

a) Comunicar el cambio de domicilio fiscal, de acuerdo con lo previsto en el artículo 48.3 de la Ley 58/2003, de 17 de diciembre, General Tributaria, por las personas jurídicas y demás entidades, así como por las personas físicas incluidas en el Censo de Empresarios, Profesionales y Retenedores.

b) Comunicar la variación de cualquiera de los datos y situaciones tributarias recogidas en los artículos 4 a 9 de este reglamento, ambos inclusive.

c) Comunicar el inicio de la realización habitual de las entregas de bienes o prestaciones de servicios correspondientes a actividades empresariales o profesionales, cuando la declaración de alta se hubiese formulado indicando que el inicio de la realización de dichas entregas de bienes o prestaciones de servicios se produciría con posterioridad al comienzo de la adquisición o importación de bienes o servicios destinados a la actividad.

Asimismo, la declaración de modificación servirá para comunicar el comienzo de la realización habitual de las entregas de bienes o prestaciones de servicios correspondientes a una nueva actividad constitutiva de un sector diferenciado a efectos del Impuesto sobre el Valor Añadido, cuando se haya presentado previamente una declaración censal mediante la que se comunique que el inicio de la realización de las entregas de bienes y prestaciones de servicios en desarrollo de dicha nueva actividad se produciría con posterioridad al comienzo de la adquisición o importación de bienes o servicios destinados a aquella.

d) Optar por la determinación de la base imponible mediante el margen de beneficio global en el régimen especial de los bienes usados, objetos de arte, antigüedades y objetos de colección a que se refiere el apartado dos del artículo 137 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.

e) Solicitar la inclusión en el Registro de operadores intracomunitarios cuando se vayan a producir, una vez presentada la declaración censal de alta, las circunstancias que lo requieran previstas en el artículo 3.3 de este reglamento.

Los sujetos pasivos del Impuesto sobre el Valor Añadido que cesen en el desarrollo de las actividades sujetas al mismo sin que ello determine su baja en el Censo de Empresarios, Profesionales y Retenedores, y las personas o entidades que durante los 12 meses anteriores no hayan realizado entregas o adquisiciones intracomunitarias de bienes sujetas al Impuesto sobre el Valor Añadido o no hayan prestado o sido destinatarios de las prestaciones de servicios a que se refieren los párrafos c) y d) del artículo 3.3 de este reglamento, deberán presentar, asimismo, una declaración censal de modificación solicitando la baja en el Registro de operadores intracomunitarios.

f) Optar por la no sujeción al Impuesto sobre el Valor Añadido de las entregas de bienes a que se refiere el artículo 68.Cuatro de la ley de dicho impuesto, en relación con lo previsto en el artículo 73 de esa ley.

g) Comunicar la sujeción al Impuesto sobre el Valor Añadido de las entregas a que se refieren el artículo 68.Tres.a) y cinco de la ley de dicho impuesto.

h) Revocar las opciones o modificar las solicitudes a que se refieren los párrafos d), e), f), p), q) y r) de este apartado y los párrafos f), h), q), r) y s) del artículo 9.3 de este Reglamento, así como la comunicación de los cambios de las situaciones a que se refieren los párrafos g) y s) de este apartado y los párrafos i), o) y t) del artículo 9.3 de este Reglamento.

i) Comunicar la adquisición o pérdida de la condición de contribuyente del Impuesto sobre Determinados Servicios Digitales a que se refiere el artículo 8 de la Ley 4/2020, de 15 de octubre, del Impuesto sobre Determinados Servicios Digitales.

j) En el caso de aquellos que, teniendo ya la condición de empresarios o profesionales por venir realizando actividades de tal naturaleza, inicien una nueva actividad empresarial o profesional constituya o no, a efectos del Impuesto sobre el Valor Añadido, un sector diferenciado respecto de las actividades que venían desarrollando con anterioridad, y se encuentren en cualesquiera de las circunstancias que se indican a continuación, para comunicar a la Administración su concurrencia:

1.º Que ejercen la opción por la regla de prorrata especial prevista en el artículo 103.dos.1.º de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.

2.º Que en los casos de inicio de actividad que constituya un sector diferenciado, el comienzo de la realización habitual de las entregas de bienes o prestaciones de servicios correspondientes a la nueva actividad se producirá con posterioridad al comienzo de la adquisición o importación de bienes o servicios destinados a su desarrollo y resulte aplicable el régimen de deducción previsto en los artículos 111, 112 y 113 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido. En este caso, la declaración contendrá también la propuesta del porcentaje provisional de deducción a que se refiere el citado artículo 111.dos de dicha ley.

k) Solicitar la inclusión en el Registro de exportadores y otros operadores económicos en régimen comercial, así como la baja en dicho registro, de acuerdo con el artículo 30 del Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre.

l) Comunicar a la Administración tributaria el cambio de periodo de liquidación en el Impuesto sobre el Valor Añadido y a efectos de las autoliquidaciones de retenciones e ingresos a cuenta del Impuesto sobre la Renta de las Personas Físicas, Impuesto sobre la Renta de no Residentes y del Impuesto sobre Sociedades por estar incluidos en el Registro de grandes empresas regulado en el artículo 3 de este reglamento, o en atención a la cuantía de su último presupuesto aprobado cuando se trate de retenedores u obligados a ingresar a cuenta que tengan la consideración de Administraciones públicas, incluida la Seguridad Social.

m) Optar o renunciar a la opción para determinar el pago fraccionado del Impuesto sobre Sociedades, de acuerdo con la modalidad prevista en el artículo 40.3 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades.

n) Renunciar a la aplicación del régimen de consolidación fiscal en el caso de los grupos fiscales que hayan ejercitado esta opción.

ñ) Optar o renunciar al régimen fiscal especial previsto en el título II de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.

o) Solicitar la rectificación de datos personales a que se refiere el artículo 2.5 de este reglamento.

p) Optar por la llevanza de los libros registro del Impuesto sobre el Valor Añadido a través de la Sede electrónica de la Agencia Estatal de Administración Tributaria de acuerdo con lo previsto en el artículo 62.6 del Reglamento del Impuesto sobre el Valor Añadido.

q) Comunicar la opción del cumplimiento de la obligación de expedir factura por los destinatarios de las operaciones o por terceros, en los términos del artículo 5.1 del Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre, en el caso de las personas y entidades a que se refiere el artículo 62.6 del Reglamento del Impuesto sobre el Valor Añadido.

r) Optar por la no sujeción al Impuesto sobre el Valor Añadido de las prestaciones de servicios a que se refiere el artículo 70.uno.8.º de la Ley de dicho impuesto en relación con lo previsto en el artículo 73 de esa ley.

s) Comunicar la sujeción al Impuesto sobre el Valor Añadido de las prestaciones de servicios a que se refiere el artículo 70.Uno.4.º.a) de la ley de dicho impuesto, siempre que el declarante no se encuentre ya registrado en el censo.

t) Comunicar otros hechos y circunstancias de carácter censal previstos en las normas tributarias o que determine la persona titular del Ministerio de Hacienda.

3. Esta declaración no será necesaria cuando la modificación de uno de los datos que figuren en el censo se haya producido por iniciativa de un órgano de la Agencia Estatal de Administración Tributaria.

4. La declaración deberá presentarse en el plazo de un mes desde que se hayan producido los hechos que determinan su presentación, salvo en los casos que se indican a continuación:

a) En los supuestos en que la normativa propia de cada tributo o la del régimen fiscal aplicable establezca plazos específicos, la declaración se presentará de conformidad con estos.

b) Las declaraciones a que se refiere el apartado 2.j).1.º de este artículo, deberán presentarse con anterioridad al momento en que se inicie la nueva actividad empresarial que vaya a constituir, a efectos del Impuesto sobre el Valor Añadido, un sector diferenciado de actividad respecto de las que se venían desarrollando con anterioridad.

c) La comunicación prevista en el apartado 2.l) de este artículo se formulará en el plazo general y, en cualquier caso, antes del vencimiento del plazo para la presentación de la primera declaración periódica afectada por la variación puesta en conocimiento de la Administración tributaria o que hubiese debido presentarse de no haberse producido dicha variación.

d) La solicitud a que se refiere el primer párrafo del apartado 2.e) de este artículo deberá presentarse con anterioridad al momento en el que se produzcan las circunstancias previstas en el artículo 3.3 de este reglamento.

e) Cuando el Ministro de Economía y Hacienda establezca un plazo especial atendiendo a las circunstancias que concurran en cada caso.

Artículo 11. *Declaración de baja en el Censo de Empresarios, Profesionales y Retenedores.*

1. Quienes cesen en el desarrollo de todo tipo de actividades empresariales o profesionales o, no teniendo la condición de empresarios o profesionales, dejen de satisfacer rendimientos sujetos a retención o ingreso a cuenta deberán presentar la correspondiente declaración mediante la que comuniquen a la Administración tributaria tal circunstancia a efectos de su baja en el Censo de Empresarios, Profesionales y Retenedores.

Asimismo, las personas jurídicas que no desarrollen actividades empresariales o profesionales deberán presentar esta declaración a efectos de su baja en el Registro de operadores intracomunitarios cuando sus adquisiciones intracomunitarias de bienes deban resultar no sujetas de acuerdo con el artículo 14 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.

2. La declaración de baja deberá presentarse en el plazo de un mes desde que se cumplan las condiciones previstas en el apartado 1 de este artículo, sin perjuicio de que la persona o entidad afectada deba presentar las declaraciones y cumplir las obligaciones tributarias que le incumban y sin que a estos efectos deba darse de alta en el censo.

En los supuestos mencionados en los artículos 39 y 40 de la Ley 58/2003, del 17 de diciembre, General Tributaria, se informará de los datos relativos a la identificación de los sucesores en la declaración de baja.

3. Cuando una sociedad o entidad se disuelva, la declaración de baja deberá ser presentada en el plazo de un mes desde que se haya realizado, en su caso, la cancelación efectiva de los correspondientes asientos en el Registro Mercantil.

Si no constaran dichos asientos, la Administración tributaria pondrá en conocimiento del Registro Mercantil la solicitud de baja para que este extienda una nota marginal en la hoja

registral de la entidad. En lo sucesivo, el Registro comunicará a la Administración tributaria cualquier acto relativo a dicha entidad que se presente a inscripción.

Igualmente, cuando le constaran a la Administración tributaria datos suficientes sobre el cese de la actividad de una entidad, lo pondrá en conocimiento del Registro Mercantil, para que este, de oficio, proceda a extender una nota marginal con los mismos efectos que los previstos en el párrafo anterior.

4. En el caso de fallecimiento del obligado tributario, los herederos deberán presentar la declaración de baja correspondiente en el plazo de seis meses desde el fallecimiento. Igualmente quedarán obligados a comunicar en el mismo plazo la modificación de la titularidad de cuantos derechos y obligaciones con trascendencia tributaria permanecieran vigentes con terceros y a presentar, en su caso, la declaración o declaraciones de alta que sean procedentes.

Artículo 12. *Especialidades en el alta y modificaciones en el Censo de Obligados Tributarios de las entidades a las que se asigne un número de identificación fiscal.*

1. La asignación a una entidad del número de identificación fiscal provisional previsto en el artículo 24 determinará su alta en el Censo de Obligados Tributarios y, siempre que se produzcan las circunstancias previstas en el artículo 3.2, su alta en el Censo de Empresarios, Profesionales y Retenedores.

2. Las variaciones posteriores al alta censal, incluidas las relativas al inicio de la actividad, domicilio, nombre y apellidos o razón social o denominación completa y número de identificación fiscal de los socios o personas o entidades que la integren, se comunicarán mediante la declaración de modificación regulada en el artículo 10. No será necesario comunicar las variaciones relativas a los socios, miembros o partícipes de las entidades una vez que se inscriban en el registro correspondiente y obtengan el número de identificación fiscal definitivo.

No obstante, las entidades sin personalidad jurídica deberán comunicar las variaciones relativas a sus socios, comuneros o partícipes, aunque hayan obtenido un número de identificación fiscal definitivo, salvo que tengan la condición de comunidades de propietarios constituidas en régimen de propiedad horizontal y estén incluidas en el Censo de Empresarios, Profesionales y Retenedores.

Igualmente, las entidades a las que se refiere el artículo 4.2.l) deberán comunicar en el plazo de un mes desde la fecha de formalización de su transmisión las modificaciones que se hayan producido respecto de los datos consignados en las declaraciones anteriores, incluidos los relativos a los socios, miembros o partícipes.

En la declaración de baja se comunicarán los sucesores tal y como se establece en el artículo 11.2 de este reglamento.

3. Las personas jurídicas y demás entidades deberán presentar copia de las escrituras o documentos que modifiquen los anteriormente vigentes, en el plazo de un mes desde la inscripción en el registro correspondiente o desde su otorgamiento si dicha inscripción no fuera necesaria, cuando las variaciones introducidas impliquen la presentación de una declaración censal de modificación o de baja.

[. . .]

TÍTULO III

Principios y disposiciones generales de la aplicación de los tributos

[. . .]

CAPÍTULO II

Principios generales de la aplicación de los tributos

[. . .]

Sección 2.ª La colaboración social en la aplicación de los tributos

[. . .]

Artículo 82. *Utilización de tecnologías informáticas y telemáticas.*

En la utilización de técnicas y medios electrónicos, informáticos o telemáticos deberá respetarse el derecho a la protección de datos de carácter personal en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo.

[. . .]

CAPÍTULO III

Normas comunes sobre actuaciones y procedimientos tributarios

Sección 1.ª Especialidades de los procedimientos administrativos en materia tributaria

[. . .]

Subsección 2.ª Tramitación de las actuaciones y procedimientos tributarios

[. . .]

Artículo 94. *Acceso a archivos y registros administrativos.*

1. Los obligados tributarios que hayan sido parte en el procedimiento podrán acceder a los registros y documentos que formen parte de un expediente concluido en los términos y con las condiciones establecidos en el artículo 99.5 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

2. El órgano que tramitó el expediente resolverá sobre la petición de acceso en el plazo máximo de un mes. Transcurrido este plazo sin que de forma expresa se responda a la petición de acceso, esta podrá entenderse desestimada.

Si la resolución fuera estimatoria se dejará constancia en el expediente de dicho acceso.

3. El derecho de acceso llevará consigo el de obtener copia de los documentos cuyo examen sea autorizado en los términos previstos en el artículo siguiente.

4. Cuando los documentos que formen el expediente estén almacenados por medios electrónicos, informáticos o telemáticos, se facilitará el acceso al interesado por dichos medios siempre que las disponibilidades técnicas lo permitan, de acuerdo con las especificaciones y garantías que se determinen y con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[. . .]

§ 48

Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social. [Inclusión parcial]

Ministerio de Empleo y Seguridad Social
«BOE» núm. 261, de 31 de octubre de 2015
Última modificación: 3 de febrero de 2021
Referencia: BOE-A-2015-11724

[. . .]

TÍTULO I

Normas generales del sistema de la Seguridad Social

[. . .]

CAPÍTULO III

Afiliación, cotización y recaudación

[. . .]

Sección 3.ª Liquidación y recaudación de las cuotas y demás recursos del sistema

[. . .]

Subsección 3.ª Recaudación en vía ejecutiva

[. . .]

Artículo 40. *Deber de información por parte de las personas y entidades sin personalidad, entidades financieras, funcionarios públicos, profesionales oficiales y autoridades.*

1. Las personas físicas o jurídicas, públicas o privadas, así como las entidades sin personalidad, estarán obligadas a proporcionar a la Tesorería General de la Seguridad Social y al Instituto Social de la Marina, cuando así lo requieran, aquellos datos, informes, antecedentes y justificantes con incidencia en las competencias de la Administración de la Seguridad Social, especialmente en el ámbito de la liquidación, control de la cotización y de recaudación de los recursos de la Seguridad Social y demás conceptos de recaudación conjunta.

Especialmente, las personas o entidades depositarias de dinero en efectivo o en cuenta, valores u otros bienes de deudores a la Seguridad Social en situación de apremio, estarán obligadas a informar a la Tesorería General de la Seguridad Social y a cumplir los requerimientos que le sean hechos por la misma en el ejercicio de sus funciones legales.

2. Las obligaciones a que se refiere el apartado anterior deberán cumplirse bien con carácter general o bien a requerimiento individualizado de los órganos competentes de la Administración de la Seguridad Social, en la forma y plazos que reglamentariamente se determinen.

3. El incumplimiento de las obligaciones establecidas en los números anteriores de este artículo no podrá ampararse en el secreto bancario.

Los requerimientos relativos a los movimientos de cuentas corrientes, depósitos de ahorro y a plazo, cuentas de préstamos y créditos y demás operaciones activas o pasivas de los bancos, cajas de ahorro, cooperativas de crédito y cuantas personas físicas o jurídicas se dediquen al tráfico bancario o crediticio, se efectuarán previa autorización del titular de la Dirección General de la Tesorería General de la Seguridad Social o, en su caso, y en las condiciones que reglamentariamente se establezcan, el titular de la Dirección Provincial de la Tesorería General de la Seguridad Social competente, y deberán precisar las operaciones objeto de investigación, los sujetos pasivos afectados y el alcance de la misma en cuanto al período de tiempo a que se refieren.

4. Los funcionarios públicos, incluidos los profesionales oficiales, están obligados a colaborar con la Administración de la Seguridad Social suministrando toda clase de información de que dispongan, siempre que sea necesaria para el cumplimiento de las funciones de la Administración de la Seguridad Social, especialmente respecto de la liquidación, control de la cotización y la recaudación de recursos de la Seguridad Social y demás conceptos de recaudación conjunta, salvo que sea aplicable:

a) El secreto del contenido de la correspondencia.

b) El secreto de los datos que se hayan suministrado a la Administración pública para una finalidad exclusivamente estadística.

c) El secreto del protocolo notarial, que abarcará los instrumentos públicos a que se refieren los artículos 34 y 35 de la Ley de 28 de mayo de 1862, del Notariado, y los relativos a cuestiones matrimoniales, con excepción de los referentes al régimen económico de la sociedad conyugal.

5. La obligación de los profesionales de facilitar información de transcendencia recaudatoria a la Administración de la Seguridad Social no alcanzará a los datos privados no patrimoniales que conozcan por razón del ejercicio de su actividad, cuya revelación atente al honor o a la intimidad personal o familiar de las personas. Tampoco alcanzará a aquellos datos confidenciales de sus clientes de los que tengan conocimiento como consecuencia de la prestación de servicios profesionales de asesoramiento o defensa.

Los profesionales no podrán invocar el secreto profesional a efectos de impedir la comprobación de su propia cotización a la Seguridad Social.

A efectos del artículo octavo, apartado uno, de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, se considerará autoridad competente al titular del Ministerio de Inclusión, Seguridad Social y Migraciones, a los titulares de los órganos y centros directivos de la Secretaría de Estado de la Seguridad Social y Pensiones y del Organismo Estatal Inspección de Trabajo y Seguridad Social así como al titular de la Dirección General y a los titulares de las direcciones provinciales de la Tesorería General de la Seguridad Social.

6. La cesión de aquellos datos de carácter personal que se deba efectuar a la Administración de la Seguridad Social conforme a lo dispuesto en este artículo o, en general, en cumplimiento del deber de colaborar con la Administración de la Seguridad Social para el desempeño de cualquiera de sus funciones, especialmente respecto de la efectiva liquidación, control de la cotización, recaudación de los recursos de la Seguridad Social y de los conceptos de recaudación conjunta con las cuotas de la Seguridad Social, no requerirá el consentimiento del afectado.

A los efectos señalados en el párrafo anterior, así como respecto de la cesión de datos de carácter no personal, las autoridades, cualquiera que sea su naturaleza, los titulares de

los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos, las agencias y las entidades públicas empresariales; las autoridades laborales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas y quienes, en general, ejerzan o colaboren en el ejercicio de funciones públicas, estarán obligados a suministrar a la Administración de la Seguridad Social cuantos datos, informes y antecedentes precise esta para el adecuado ejercicio de cualquiera de las funciones de la Administración de la Seguridad Social, especialmente respecto de sus funciones liquidatorias, de control de la cotización y recaudatorias, mediante disposiciones de carácter general o a través de requerimientos concretos y a prestarle, a ella y a su personal, apoyo, concurso, auxilio y protección para el ejercicio de sus competencias.

La cesión de datos a que se refiere este artículo se instrumentará preferentemente por medios informáticos. A tal efecto la Administración de la Seguridad Social podrá recabar a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas habilitados al efecto, los datos o la información necesaria para la tramitación de los procedimientos que resulten de su competencia.

7. Los datos, informes y antecedentes suministrados conforme a lo dispuesto en este artículo únicamente serán tratados en el marco de las funciones de la Administración de la Seguridad Social, especialmente en el ámbito de control de la cotización y de recaudación de los recursos del sistema de Seguridad Social, así como de sus funciones estadísticas, sin necesidad del consentimiento de los afectados y sin perjuicio de lo dispuesto en el artículo 77 de esta ley.

[. . .]

CAPÍTULO IV

Acción protectora

[. . .]

Sección 3.ª Prescripción, caducidad y reintegro de prestaciones indebidas

[. . .]

Subsección 2.ª Pensiones contributivas

[. . .]

Artículo 60. *Complemento de pensiones contributivas para la reducción de la brecha de género.*

1. Las mujeres que hayan tenido uno o más hijos o hijas y que sean beneficiarias de una pensión contributiva de jubilación, de incapacidad permanente o de viudedad, tendrán derecho a un complemento por cada hijo o hija, debido a la incidencia que, con carácter general, tiene la brecha de género en el importe de las pensiones contributivas de la Seguridad Social de las mujeres. El derecho al complemento por cada hijo o hija se reconocerá o mantendrá a la mujer siempre que no medie solicitud y reconocimiento del complemento en favor del otro progenitor y si este otro es también mujer, se reconocerá a aquella que perciba pensiones públicas cuya suma sea de menor cuantía.

Para que los hombres puedan tener derecho al reconocimiento del complemento deberá concurrir alguno de los siguientes requisitos:

a) Causar una pensión de viudedad por fallecimiento del otro progenitor por los hijos o hijas en común, siempre que alguno de ellos tenga derecho a percibir una pensión de orfandad.

b) Causar una pensión contributiva de jubilación o incapacidad permanente y haber interrumpido o haber visto afectada su carrera profesional con ocasión del nacimiento o adopción, con arreglo a las siguientes condiciones:

1.ª En el supuesto de hijos o hijas nacidos o adoptados hasta el 31 de diciembre de 1994, tener más de ciento veinte días sin cotización entre los nueve meses anteriores al nacimiento y los tres años posteriores a dicha fecha o, en caso de adopción, entre la fecha de la resolución judicial por la que se constituya y los tres años siguientes, siempre que la suma de las cuantías de las pensiones reconocidas sea inferior a la suma de las pensiones que le corresponda a la mujer.

2.ª En el supuesto de hijos o hijas nacidos o adoptados desde el 1 de enero de 1995, que la suma de las bases de cotización de los veinticuatro meses siguientes al del nacimiento o al de la resolución judicial por la que se constituya la adopción sea inferior, en más de un 15 por ciento, a la de los veinticuatro meses inmediatamente anteriores, siempre que la cuantía de las sumas de las pensiones reconocidas sea inferior a la suma de las pensiones que le corresponda a la mujer.

3.ª Si los dos progenitores son hombres y se dan las condiciones anteriores en ambos, se reconocerá a aquel que perciba pensiones públicas cuya suma sea de menor cuantía.

4.ª El requisito, para causar derecho al complemento, de que la suma de las pensiones reconocidas sea inferior a la suma de las pensiones que le corresponda al otro progenitor, se exigirá en el momento en que ambos progenitores causen derecho a una prestación contributiva en los términos previstos en la norma.

2. El reconocimiento del complemento al segundo progenitor supondrá la extinción del complemento ya reconocido al primer progenitor y producirá efectos económicos el primer día del mes siguiente al de la resolución, siempre que la misma se dicte dentro de los seis meses siguientes a la solicitud o, en su caso, al reconocimiento de la pensión que la cause; pasado este plazo, los efectos se producirán desde el primer día del séptimo mes.

Antes de dictar la resolución reconociendo el derecho al segundo progenitor se dará audiencia al que viniera percibiendo el complemento.

3. Este complemento tendrá a todos los efectos naturaleza jurídica de pensión pública contributiva.

El importe del complemento por hijo o hija se fijará en la correspondiente Ley de Presupuestos Generales del Estado. La cuantía a percibir estará limitada a cuatro veces el importe mensual fijado por hijo o hija y será incrementada al comienzo de cada año en el mismo porcentaje previsto en la correspondiente Ley de Presupuestos Generales del Estado para las pensiones contributivas.

La percepción del complemento estará sujeta además a las siguientes reglas:

a) Cada hijo o hija dará derecho únicamente al reconocimiento de un complemento.

A efectos de determinar el derecho al complemento, así como su cuantía, únicamente se computarán los hijos o hijas que con anterioridad al hecho causante de la pensión correspondiente hubieran nacido con vida o hubieran sido adoptados.

b) No se reconocerá el derecho al complemento al padre o a la madre que haya sido privado de la patria potestad por sentencia fundada en el incumplimiento de los deberes inherentes a la misma o dictada en causa criminal o matrimonial.

Tampoco se reconocerá el derecho al complemento al padre que haya sido condenado por violencia contra la mujer, en los términos que se defina por la ley o por los instrumentos internacionales ratificados por España, ejercida sobre la madre, ni al padre o a la madre que haya sido condenado o condenada por ejercer violencia contra los hijos o hijas.

c) El complemento será satisfecho en catorce pagas, junto con la pensión que determine el derecho al mismo.

d) El importe del complemento no será tenido en cuenta en la aplicación del límite máximo de pensiones previsto en los artículos 57 y 58.7.

e) El importe de este complemento no tendrá la consideración de ingreso o rendimiento de trabajo en orden a determinar si concurren los requisitos para tener derecho al complemento por mínimos previsto en el artículo 59. Cuando concurran dichos requisitos, se reconocerá la cuantía mínima de pensión según establezca anualmente la correspondiente Ley de Presupuestos Generales del Estado. A este importe se sumará el complemento para la reducción de la brecha de género.

f) Cuando la pensión contributiva que determina el derecho al complemento se cause por totalización de períodos de seguro a *prorrata temporis* en aplicación de normativa

internacional, el importe real del complemento será el resultado de aplicar a la cuantía a la que se refiere el apartado anterior, que será considerada importe teórico, la prorrata aplicada a la pensión a la que acompaña.

4. No se tendrá derecho a este complemento en los casos de jubilación parcial, a la que se refiere el artículo 215 y el apartado sexto de la disposición transitoria cuarta.

No obstante, se reconocerá el complemento que proceda cuando desde la jubilación parcial se acceda a la jubilación plena, una vez cumplida la edad que en cada caso corresponda.

5. Sin perjuicio de lo dispuesto en el apartado 2, el complemento se abonará en tanto la persona beneficiaria perciba una de las pensiones citadas en el apartado 1. En consecuencia, su nacimiento, suspensión y extinción coincidirá con el de la pensión que haya determinado su reconocimiento. No obstante, cuando en el momento de la suspensión o extinción de dicha pensión la persona beneficiaria tuviera derecho a percibir otra distinta, de entre las previstas en el apartado 1, el abono del complemento se mantendrá, quedando vinculado al de esta última.

6. Los complementos que pudieran ser reconocidos en cualquiera de los regímenes de Seguridad Social serán incompatibles entre sí, siendo abonado en el régimen en el que el causante de la pensión tenga más periodos de alta.

[. . .]

CAPÍTULO V

Gestión de la Seguridad Social

Sección 1.ª Entidades gestoras

[. . .]

Artículo 71. *Suministro de información a la Administración de la Seguridad Social.*

1. Se establecen los siguientes supuestos de suministro de información a la Administración de la Seguridad Social:

a) Por los organismos competentes dependientes del Ministerio de Hacienda o, en su caso, de las comunidades autónomas o de las diputaciones forales, se facilitarán, dentro de cada ejercicio anual, conforme al artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria y normativa foral equivalente, a las entidades gestoras de la Seguridad Social responsables de la gestión de las prestaciones económicas y, a petición de las mismas, los datos relativos a los niveles de renta, patrimonio y demás ingresos o situaciones de los titulares de prestaciones en cuanto determinen el derecho a las mismas, así como de los beneficiarios, cónyuges y otros miembros de las unidades familiares, siempre que deban tenerse en cuenta para el reconocimiento, mantenimiento o cuantía de dichas prestaciones a fin de verificar si aquellos cumplen en todo momento las condiciones necesarias para la percepción de las prestaciones y en la cuantía legalmente establecida.

Asimismo, facilitarán a las entidades gestoras de Seguridad Social que gestionen ayudas o subvenciones públicas, la información sobre el cumplimiento de las obligaciones tributarias, así como los datos relativos a las inhabilitaciones para obtener este tipo de ayudas o subvenciones y a la concesión de las mismas que deban tenerse en cuenta para el reconocimiento del derecho o el importe de las ayudas o subvenciones a conceder.

b) El organismo que designe el Ministerio de Justicia facilitará a las entidades gestoras de la Seguridad Social la información que estas soliciten acerca de las inscripciones y datos que guarden relación con el nacimiento, modificación, conservación o extinción del derecho a las prestaciones económicas de la Seguridad Social.

Además, el encargado del Registro Central de Penados y el del Registro de Medidas Cautelares, Requisitorias y Sentencias no Firmes comunicará al menos semanalmente a las entidades gestoras de la Seguridad Social los datos relativos a penas, medidas de seguridad y medidas cautelares impuestas por existir indicios racionales de criminalidad por la comisión de un delito doloso de homicidio en cualquiera de sus formas, cuando la víctima fuera

ascendiente, descendiente, hermano, cónyuge o ex cónyuge del investigado, o estuviera o hubiese estado ligada a él por una relación de afectividad análoga a la conyugal. Estas comunicaciones se realizarán a los efectos de lo previsto en los artículos 231, 232, 233 y 234 de la presente ley; en los artículos 37 bis y 37 ter del texto refundido de la Ley de Clases Pasivas del Estado, aprobado por el Real Decreto Legislativo 670/1987, de 30 de abril, y en los artículos 4, 5, 6, 7 y 10 del Real Decreto-ley 20/2020, de 29 de mayo, por el que se establece el ingreso mínimo vital.

c) Los empresarios facilitarán a las entidades gestoras de la Seguridad Social los datos que estas les soliciten, por vía telemática siempre que esté habilitado un canal para su remisión informática, con el fin de poder efectuar las comunicaciones a través de sistemas electrónicos que garanticen un procedimiento de comunicación ágil en el reconocimiento y control de las prestaciones de la Seguridad Social relativas a sus trabajadores.

Los datos que se faciliten en relación con los trabajadores deberán identificar, en todo caso, nombre y apellidos, documento nacional de identidad o número de identificación de extranjero y domicilio.

d) Por el Instituto Nacional de Estadística se facilitarán a las entidades gestoras de la Seguridad Social responsables de la gestión de las prestaciones económicas, así como de la formación marítima y sanitaria de los trabajadores del mar, los datos de domicilio relativos al Padrón municipal referidos al periodo que se requiera, comprendiendo, en su caso, los del padrón histórico y/o colectivo del domicilio, así como dónde residen o han residido los ciudadanos, cuando dichos datos puedan guardar relación con el nacimiento, modificación, conservación o extinción del derecho a dichas prestaciones en cualquier procedimiento, así como con la actualización de la información obrante en las bases de datos del sistema de Seguridad Social.

e) El Ministerio del Interior facilitará a las entidades gestoras de la Seguridad Social por medios informáticos las fechas de concesión, prórroga o modificación de las situaciones de las personas extranjeras en España, de renovación, recuperación o, en su caso, extinción de las autorizaciones de residencia, y sus efectos, así como los movimientos fronterizos de las personas que tengan derecho a una prestación para cuya percepción sea necesario el cumplimiento del requisito de residencia efectiva en España.

Asimismo, facilitará a las entidades gestoras de la Seguridad Social por medios informáticos los datos incorporados en el Documento Nacional de Identidad o, en el caso de extranjeros, documentación de identidad equivalente de las personas, cuyos datos tengan trascendencia en procedimientos seguidos ante dichas entidades gestoras.

f) Las mutuas colaboradoras con la Seguridad Social facilitarán telemáticamente a las entidades gestoras responsables de la gestión de las prestaciones económicas de la Seguridad Social los datos que puedan afectar al nacimiento, modificación, conservación o extinción del derecho a las prestaciones y los importes de las mismas que sean reconocidas por aquellas. Asimismo, facilitaran a la Dirección General de Ordenación de la Seguridad Social los datos que puedan afectar a la prestación por cese de actividad cuando así sea requerido para ello.

g) El Instituto de Mayores y Servicios Sociales y los organismos competentes de las comunidades autónomas facilitarán a las entidades gestoras de la Seguridad Social los datos de grado y nivel de dependencia y los datos incluidos en los certificados de discapacidad que puedan guardar relación con el nacimiento, modificación, conservación o extinción del derecho a las prestaciones en cualquier procedimiento, así como con la actualización de la información obrante en las bases de datos del sistema de Seguridad Social y en el sistema de información Tarjeta Social Digital.

Con la misma finalidad, facilitarán los datos de los beneficiarios, importes y fecha de efectos de concesión, modificación o extinción, de las prestaciones económicas previstas en la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia.

Sin perjuicio de lo previsto en el párrafo anterior, el Instituto de Mayores y Servicios Sociales suministrará al Instituto Nacional de la Seguridad Social la información relativa a las mencionadas prestaciones económicas que figure en el sistema de información del Sistema para la Autonomía y Atención a la Dependencia, previsto en el artículo 37 de la Ley 39/2006, de 14 de diciembre.

h) Las comunidades autónomas facilitarán a las entidades gestoras de la Seguridad Social por medios informáticos los datos relativos a las fechas de reconocimiento y vencimiento de los títulos de familias numerosas, así como los datos relativos a los miembros de la unidad familiar incluidos en los mismos, que puedan guardar relación con el nacimiento, modificación, conservación o extinción del derecho a las prestaciones en cualquier procedimiento, así como con la actualización de la información obrante en las bases de datos del sistema.

Asimismo, facilitarán a las entidades gestoras de Seguridad Social que gestionen ayudas o subvenciones públicas, los datos sobre el cumplimiento de las obligaciones tributarias que deban tenerse en cuenta para el reconocimiento del derecho o el importe de las ayudas o subvenciones a conceder.

Por otra parte, facilitarán a la entidad gestora del Régimen Especial de la Seguridad Social de los Trabajadores del Mar los datos sobre el permiso de explotación marisquera, que puedan guardar relación con la incorporación de los trabajadores dedicados al marisqueo en el citado Régimen Especial.

i) La Dirección General de la Marina Mercante facilitará a la entidad gestora del Régimen Especial de la Seguridad Social de los Trabajadores del Mar los datos sobre las titulaciones correspondientes a los trabajadores embarcados que puedan guardar relación con el acceso a la formación marítima prestada por dicha entidad.

j) Las mutualidades de previsión social alternativas al Régimen Especial de la Seguridad Social de los Trabajadores por Cuenta Propia o Autónomos y los colegios profesionales, facilitarán a la Administración de la Seguridad Social, cuando así se le solicite, los datos de los profesionales colegiados que puedan afectar a las prestaciones, así como a la afiliación, alta, baja y variación de datos y cotización.

2. Todos los datos relativos a los solicitantes de prestaciones económicas del Sistema de Seguridad Social que obren en poder de las entidades gestoras y que hayan sido remitidos por otros organismos públicos o por empresas mediante transmisión telemática, o cuando aquellos se consoliden en las bases de datos corporativas del sistema de la Seguridad Social como consecuencia del acceso electrónico directo a las bases de datos corporativas de otros organismos o empresas, surtirán plenos efectos y tendrán la misma validez que si hubieran sido notificados por dichos organismos o empresas mediante certificación en soporte papel.

Los suministros de información a las entidades gestoras de la Seguridad Social mencionados en este apartado y en el anterior no precisarán consentimiento previo del interesado.

Los datos, informes y antecedentes suministrados conforme a lo dispuesto en este apartado y en el anterior únicamente serán tratados en el marco de las funciones de gestión de prestaciones atribuidas a las entidades gestoras y servicios comunes de la Seguridad Social, sin perjuicio de lo dispuesto en el artículo 77.

3. En los procedimientos de declaración y revisión de la incapacidad permanente, a efectos de las correspondientes prestaciones económicas de la Seguridad Social, así como en lo que respecta al reconocimiento y control de las prestaciones por incapacidad temporal, orfandad o asignaciones familiares por hijo a cargo, las instituciones sanitarias, las mutuas colaboradoras con la Seguridad Social y las empresas colaboradoras remitirán a las entidades gestoras de la Seguridad Social los informes, la historia clínica y demás datos médicos, relacionados con las lesiones y dolencias padecidas por el interesado que resulten relevantes para la resolución del procedimiento.

Los inspectores médicos adscritos al Instituto Nacional de la Seguridad Social, en el ejercicio de sus funciones, cuando sea necesario para el reconocimiento y control del percibo de las prestaciones de los trabajadores pertenecientes al sistema de la Seguridad Social, y para la determinación de contingencia, así como los médicos de sanidad marítima adscritos al Instituto Social de la Marina, para llevar a cabo los reconocimientos médicos de embarque marítimo, informando de estas actuaciones, y en los términos y condiciones que se acuerden entre el Instituto Nacional de la Seguridad Social y los Servicios de Salud de las Comunidades Autónomas y el Instituto Nacional de Gestión Sanitaria, tendrán acceso electrónico y en papel a la historia clínica de dichos trabajadores, existente en los servicios

públicos de salud, en las mutuas colaboradoras con la Seguridad Social, en las empresas colaboradoras y en los centros sanitarios privados.

Las entidades gestoras de la Seguridad Social, en el ejercicio de sus competencias de reconocimiento y control de las prestaciones, recibirán los partes médicos de incapacidad temporal expedidos por los servicios públicos de salud, las mutuas colaboradoras con la Seguridad Social y las empresas colaboradoras, a efectos del tratamiento de los datos contenidos en los mismos. Asimismo, las entidades gestoras y las entidades colaboradoras con la Seguridad Social podrán facilitarse, recíprocamente, los datos relativos a las beneficiarias que resulten necesarios para el reconocimiento y control de las prestaciones por riesgo durante el embarazo y riesgo durante la lactancia natural.

La inspección médica de los servicios públicos de salud tendrá acceso electrónico a los datos médicos necesarios para el ejercicio de sus competencias, que obren en poder de las entidades gestoras de la Seguridad Social.

En los supuestos previstos en este apartado no será necesario recabar el consentimiento del interesado, de conformidad con lo dispuesto en los artículos 6.1. e) y 9.2 h), del Reglamento (UE 2016/679) del Parlamento y el Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

4. Reglamentariamente se determinará la forma en que se remitirán a las entidades encargadas de la gestión de las pensiones de la Seguridad Social los datos que aquellas requieran para el cumplimiento de sus funciones.

[. . .]

Sección 3.ª Normas comunes a las entidades gestoras y servicios comunes

[. . .]

Artículo 77. *Reserva de datos.*

1. Los datos, informes o antecedentes obtenidos por la Administración de la Seguridad Social en el ejercicio de sus funciones tienen carácter reservado y solo podrán utilizarse para los fines encomendados a las distintas entidades gestoras, servicios comunes y órganos que integran la Administración de la Seguridad Social, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión o comunicación tenga por objeto:

a) La investigación o persecución de delitos públicos por los órganos jurisdiccionales, el Ministerio Público o la Administración de la Seguridad Social.

b) La colaboración con las Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.

c) La colaboración con la Intervención General de la Seguridad Social, en el ejercicio de su control interno o con las demás entidades gestoras y servicios comunes de la Seguridad Social, distintas del cedente y demás órganos de la Administración de la Seguridad Social.

d) La colaboración con cualesquiera otras administraciones públicas para la lucha contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos, incluidos los de la Unión Europea, para la obtención o percepción de prestaciones incompatibles en los distintos regímenes del sistema de la Seguridad Social y, en general, para el ejercicio de las funciones encomendadas legal o reglamentariamente a las mismas para las que los datos obtenidos por la Administración de la Seguridad Social resulten relevantes.

e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.

f) La protección de los derechos e intereses de los menores o personas con capacidad modificada por los órganos jurisdiccionales o el Ministerio Público.

g) La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Administración de la Seguridad Social.

h) La colaboración con los jueces y tribunales en el curso del proceso y para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución

expresa, en la que, por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración de la Seguridad Social.

i) La colaboración con el Organismo Estatal Inspección de Trabajo y Seguridad Social en el ejercicio de sus funciones de inspección. El Organismo Estatal Inspección de Trabajo y Seguridad Social tendrá acceso directo a los datos, informes y antecedentes obtenidos por la Administración de la Seguridad Social en el ejercicio de sus funciones, que resulten necesarios para la preparación y ejercicio de sus funciones de inspección.

j) La colaboración con el organismo autónomo Jefatura Central de Tráfico para que este inicie, en su caso, el procedimiento de declaración de pérdida de vigencia del permiso o la licencia de conducción de vehículo a motor por incumplimiento de los requisitos para su otorgamiento en aquellos supuestos en que el Instituto Nacional de la Seguridad Social declare en situación de incapacidad permanente a un trabajador profesional de la conducción como consecuencia de presentar una limitación orgánica y/o funcional que disminuya o anule su capacidad de conducción de vehículos a motor.

La colaboración se realizará mediante un aviso, en el que no se harán constar otros datos relativos a la salud del trabajador afectado.

k) La finalidad de facilitar la información que sea estrictamente necesaria para el reconocimiento y control de las prestaciones de carácter social competencia de las Comunidades Autónomas y entidades locales, a través de la adhesión a los procedimientos informáticos y con los requisitos de tratamiento de la información establecidos por la correspondiente entidad gestora. La información facilitada no podrá ser utilizada con ninguna otra finalidad si no es con el consentimiento del interesado.

l) La colaboración con cualesquiera otras administraciones públicas para el suministro e intercambio de datos en materia de Seguridad Social para fines de estadística pública en los términos de la legislación reguladora de dicha función pública.

m) Fines de investigación científica en el ámbito de la protección social, en el marco establecido por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), incluidas las posibles comunicaciones instrumentales que, a efectos de la realización de la investigación, resulte preciso efectuar a sujetos distintos de aquellos que lleven a cabo directamente dicha investigación. Se entenderán comprendidas en esta finalidad las actividades de evaluación de las políticas públicas en materia de protección social.

Los tratamientos que se efectúen en relación con esta finalidad se limitarán a los datos estrictamente imprescindibles para la realización de la actividad de que se trate, utilizándose los procedimientos adecuados que no permitan la identificación de los interesados. Ello no impedirá la comunicación de datos sin anonimizar a efectos meramente instrumentales cuando ello resulte imprescindible para realizar la actividad, se limite a los datos estrictamente necesarios, se garantice que el encargado del tratamiento no podrá utilizarlos con otra finalidad y el tratamiento ulterior garantice la no identificación de los interesados.

El tratamiento de los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 únicamente se efectuará cuando exista consentimiento expreso de los afectados.

n) La colaboración con la Dirección General de la Marina Mercante para el control de la situación de alta en la Seguridad Social y respecto al reconocimiento médico de embarque marítimo de los tripulantes y de los botiquines de las embarcaciones en el ejercicio de las funciones que tiene encomendadas en relación con el despacho de buques.

Los datos, informes o antecedentes a los que se refiere este apartado se cederán o comunicarán a través de medios electrónicos, salvo que, a criterio de la Administración de la Seguridad Social, por la naturaleza de los informes o antecedentes no puedan utilizarse tales medios. La entidad gestora, servicio común u órgano que ceda o comunique estos datos, informes o antecedentes, establecerá los procedimientos y datos a través de los cuales se debe realizar dicha cesión o comunicación.

2. El acceso a los datos, informes o antecedentes de todo tipo obtenidos por la Administración de la Seguridad Social sobre personas físicas o jurídicas, cualquiera que sea

su soporte, por el personal al servicio de aquella y para fines distintos de las funciones que le son propias, se considerará siempre falta disciplinaria grave.

3. Cuantas autoridades y personal al servicio de la Administración de la Seguridad Social tengan conocimiento de estos datos o informes estarán obligados al más estricto y completo sigilo respecto de ellos, salvo en los casos de los delitos citados, en los que se limitarán a deducir el tanto de culpa o a remitir al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito. Con independencia de las responsabilidades penales o civiles que pudieran corresponder, la infracción de este particular deber de sigilo se considerará siempre falta disciplinaria muy grave.

[. . .]

§ 49

Orden INT/3022/2010, de 23 de noviembre, por la que se regula el Tablón Edictal de Sanciones de Tráfico

Ministerio del Interior
«BOE» núm. 285, de 25 de noviembre de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-18102

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, ha venido a consagrar la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para dichas Administraciones.

La citada Ley, en su artículo 12, establece que la publicación de actos y comunicaciones que, por disposición legal o reglamentaria, deban publicarse en tablón de anuncios o edictos, podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente. La sede electrónica del Organismo Autónomo Jefatura Central de Tráfico ha sido aprobada mediante Resolución de la Dirección General de Tráfico de 11 de marzo de 2010.

En este contexto, la Ley 18/2009, de 23 de noviembre, por la que se modifica el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 339/1990, de 2 de marzo, en materia sancionadora, crea el Tablón Edictal de Sanciones de Tráfico, en formato digital, que se constituye en un tablón de anuncios o edictos, conforme se establece en el citado artículo 12 de la Ley 11/2007, de 22 de junio.

La notificación a través del Tablón Edictal de Sanciones de Tráfico será única, de manera que todas las notificaciones a que den lugar los procedimientos sancionadores en materia de tráfico, en el caso de que no hayan podido ser notificadas al interesado en su domicilio o en su Dirección Electrónica Vial, tendrán que publicarse en dicho Tablón y sustituirá a la notificación mediante edictos que actualmente se lleva a cabo por medio de anuncios en el tablón de edictos del Ayuntamiento, en el «Boletín Oficial del Estado», de la Comunidad Autónoma o de la Provincia, conforme a lo dispuesto en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Además, de acuerdo con lo dispuesto en el artículo 78 de dicho texto articulado, el Tablón Edictal de Sanciones de Tráfico será gestionado por la Dirección General de Tráfico y la práctica de la notificación en el mismo se efectuará en los términos que se determinen por orden del Ministro del Interior.

Esta previsión debe tener efecto desde el día 25 de noviembre de 2010, según se establece en la disposición final séptima de la Ley 18/2009, de 23 de noviembre, fecha a partir de la cual todas las notificaciones del procedimiento sancionador en materia de tráfico

que no se hayan podido practicar en la Dirección Electrónica Vial o en el domicilio del interesado, se publicarán en el Tablón Edictal de Sanciones de Tráfico.

El objetivo principal de esta orden es dar cumplimiento a ese mandato legal estableciendo el funcionamiento, la gestión y la publicación en el Tablón Edictal de Sanciones de Tráfico, con pleno sometimiento a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y conforme a los requisitos exigidos por la Ley 11/2007, de 22 de junio, dotándolo de plena autenticidad y validez jurídica.

De su contenido cabe destacar el carácter universal y gratuito de la consulta al Tablón Edictal de Sanciones de Tráfico, que será libremente accesible a través de Internet a todos los ciudadanos conforme al principio de igualdad consagrado en el articulo 4.b) de la citada Ley 11/2007, de 22 de junio, de manera que ningún ciudadano pueda sentirse discriminado por el hecho de no disponer de los medios electrónicos necesarios.

Se establecen, para ello, puntos de acceso en oficinas públicas, modalidades varias de apoyo y asistencia a la búsqueda de documentos, así como, en todo caso, la posibilidad, al alcance de todo ciudadano, de obtener una copia impresa en papel de los edictos que se hayan publicado en el Tablón Edictal de Sanciones de Tráfico.

La presente orden ha sido informada favorablemente por la Comisión Ministerial de Administración Electrónica conforme a lo dispuesto en el párrafo l) del apartado segundo de la Orden INT/3192/2008, de 4 de noviembre, por la que se regula la composición y funciones de la citada Comisión.

Asimismo, ha sido informada por la Agencia Española de Protección de Datos, de acuerdo con lo dispuesto en el artículo 5.b) del Estatuto de la citada Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo.

En su virtud, con la aprobación previa de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, de acuerdo con el Consejo de Estado, dispongo:

Artículo 1. *Objeto.*

1. La presente orden tiene por objeto regular el Tablón Edictal de Sanciones de Tráfico como medio oficial de publicación a través de edictos de las notificaciones a que dé lugar el procedimiento sancionador como consecuencia de la comisión de infracciones a la normativa sobre tráfico, circulación de vehículos a motor y seguridad vial, que no se hayan podido practicar en la Dirección Electrónica Vial, en las equivalentes de las Comunidades Autónomas con competencias ejecutivas en materia de tráfico, o en el domicilio del interesado, para cuya sanción sean competentes:

a) Los Jefes Provinciales y Locales de Tráfico.

b) Los órganos correspondientes de las Comunidades Autónomas con competencias ejecutivas en materia de tráfico.

c) Los Alcaldes.

2. Asimismo, se publicarán en él las notificaciones de las resoluciones de los recursos administrativos interpuestos contra las resoluciones sancionadoras a que se refiere el apartado anterior, con independencia de cuál sea la autoridad sancionadora competente.

3. La publicación en el Tablón Edictal de Sanciones de Tráfico tendrá la consideración de oficial y auténtica, con arreglo a las normas y condiciones que se establecen en la presente orden.

Artículo 2. *Características del Tablón Edictal de Sanciones de Tráfico.*

1. El Tablón Edictal de Sanciones de Tráfico será de formato digital y se ajustará a las especificaciones que se establecen en esta orden, así como a las condiciones establecidas en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y en su normativa de desarrollo.

2. Se publicará en la sede electrónica del Organismo Autónomo Jefatura Central de Tráfico siendo accesible en dicha sede las veinticuatro horas del día, todos los días del año, salvo que resulte imposible por circunstancias extraordinarias de carácter técnico.

3. La publicación en el Tablón Edictal de Sanciones de Tráfico, respetará los principios de accesibilidad y facilidad de uso, de acuerdo con las normas establecidas al respecto,

utilizará estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos, con una constante adaptación al progreso tecnológico.

En particular, tendrá las condiciones de accesibilidad que faciliten su consulta por las personas con discapacidad o de edad avanzada, de acuerdo con lo establecido en el Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

Artículo 3. *Garantías del Tablón Edictal de Sanciones de Tráfico.*

1. La Dirección General de Tráfico como órgano gestor del Tablón Edictal de Sanciones de Tráfico será responsable de:

a) Garantizar la autenticidad e integridad de su contenido y de los edictos que en él se publiquen mediante el empleo de los sistemas de firma electrónica relacionados en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

A tal efecto, en la Dirección General de Tráfico existirán los registros de firmas electrónicas de los organismos emisores facultados para firmar la solicitud de publicación en el Tablón Edictal de Sanciones de Tráfico.

b) Velar para que reúna las condiciones de accesibilidad necesarias para su consulta por las personas con discapacidad o de edad avanzada y su permanente adaptación al progreso tecnológico.

c) Garantizar, mediante el empleo de los medios técnicos adecuados, la generación del código seguro de verificación que garantice la integridad del edicto publicado.

d) Garantizar a través de redes públicas de telecomunicación, el acceso universal y gratuito al Tablón Edictal de Sanciones de Tráfico, con respeto a las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, e implantar en el Tablón Edictal de Sanciones de Tráfico las medidas de seguridad establecidas en la citada Ley Orgánica y su normativa de desarrollo.

e) Publicar en la sede electrónica del Organismo Autónomo Jefatura Central de Tráfico las prácticas y procedimientos necesarios para la efectividad de lo previsto en este artículo.

2. Los ciudadanos podrán verificar el cumplimiento de estas exigencias mediante aplicaciones estándar o, en su caso, mediante las herramientas informáticas que proporcione la sede electrónica del Organismo Autónomo Jefatura Central de Tráfico.

Artículo 4. *Acceso de los ciudadanos al Tablón Edictal de Sanciones de Tráfico.*

1. Los ciudadanos tendrán acceso libre y gratuito al Tablón Edictal de Sanciones de Tráfico, sin necesidad de utilizar ningún mecanismo de identificación y autenticación.

2. La Dirección General de Tráfico ofrecerá en la sede electrónica del Organismo Autónomo Jefatura Central de Tráfico un sistema de búsqueda avanzado que permitirá a los ciudadanos localizar si tienen edictos publicados en el Tablón Edictal de Sanciones de Tráfico, así como su recuperación e impresión, tanto de los que se encuentren dentro del plazo de publicación como de aquéllos en los que dicho plazo haya concluido. Dicho sistema de búsqueda avanzado contará con los mecanismos necesarios para evitar la indexación y recuperación automática de publicaciones a través de motores de búsqueda desde Internet.

La conservación y almacenamiento de la información obtenida como consecuencia de la consulta del Tablón Edictal de Sanciones de Tráfico, únicamente le estará permitida al propio interesado, a la persona a la que éste hubiera autorizado y a las Administraciones Públicas que por Ley lo tengan autorizado, resultando en los restantes casos contraria a lo dispuesto en el artículo 7.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En las oficinas de información y atención al ciudadano de la Administración General del Estado, así como en las equivalentes de la Administración Local de los organismos que envíen edictos para su publicación en el Tablón Edictal de Sanciones de Tráfico, se facilitará la consulta pública y gratuita a éste. Con ese fin, en cada una de ellas existirá, al menos, un terminal informático a través del cuál se podrán realizar búsquedas en el Tablón Edictal de Sanciones de Tráfico. Dichas oficinas deberán facilitar a las personas que lo soliciten una copia impresa de los edictos que requieran.

Artículo 5. *Lista de excluidos.*

1. Los ciudadanos que no deseen que sus datos de carácter personal incluidos en los edictos publicados puedan ser visualizados por cualquier usuario que acceda al Tablón Edictal de Sanciones de Tráfico, podrán solicitar el alta en el servicio «lista de excluidos».

2. El alta en el servicio «lista de excluidos» supondrá que los datos personales contenidos en los edictos publicados en el Tablón Edictal de Sanciones de Tráfico, sólo podrán ser visualizados por el propio interesado y por las personas a las cuáles éste haya autorizado, sin que por ello se vea afectada la autenticidad y validez del edicto original.

3. No obstante lo dispuesto en los apartados anteriores, el Defensor del Pueblo, el Ministerio Fiscal, la Agencia Estatal de Administración Tributaria o los órganos equivalentes de la Administración Autonómica o Local, los Jueces y Tribunales, así como el organismo emisor del edicto, podrán acceder a los datos de carácter personal contenidos en los edictos de los ciudadanos que estén dados de alta en la «lista de excluidos».

4. El alta y la baja en el servicio se solicitará a través de la aplicación informática que la Dirección General de Tráfico pondrá a disposición de los ciudadanos en la sede electrónica del Organismo Autónomo Jefatura Central de Tráfico, surtirá efectos desde las veinticuatro horas siguientes a la solicitud y afectará a todos los edictos publicados en el Tablón Edictal de Sanciones de Tráfico, tanto si se encuentran en estado vigente como si están en estado no vigente.

5. Para solicitar el alta o la baja en el servicio, así como para poder visualizar los datos de carácter personal contenidos en los edictos de aquellos ciudadanos que estén dados de alta en la «lista de excluidos», se exigirá identificación y autenticación mediante los sistemas de firma electrónica relacionados en el artículo 13.2.a) y b) de la Ley 11/2007, de 22 de junio.

Artículo 6. *Características de los edictos.*

1. En la cabecera de cada edicto, así como en la de cada una de sus páginas, figurará:

a) El escudo de España.
b) La denominación «Tablón Edictal de Sanciones de Tráfico».
c) El logo del Tablón Edictal de Sanciones de Tráfico.
d) El número del organismo emisor.
e) La fecha de publicación.
f) El número de página.

2. Al inicio del edicto figurará, además, la identificación del organismo emisor y, opcionalmente, su escudo.

3. En el pie de cada página del edicto, se incluirá la dirección de la sede electrónica, la denominación «Tablón Edictal de Sanciones de Tráfico», así como el logo de la Dirección General de Tráfico.

4. En todas las páginas de cada edicto que se publique se incluirá el código seguro de verificación que permita contrastar su autenticidad.

5. La fecha de publicación de cada edicto será la que figure en la cabecera y en cada una de las páginas del edicto que se inserte.

6. Todos los edictos figurarán numerados de manera correlativa por cada organismo que solicite la publicación y año.

Artículo 7. *Competencias para la inserción de edictos.*

Corresponde a la Dirección General de Tráfico la ordenación y control de la inserción de los edictos en el Tablón Edictal de Sanciones de Tráfico, tanto de los propios como de los de las otras Administraciones con competencia sancionadora en materia de tráfico, velando por el cumplimiento de los requisitos formales necesarios en cada caso, sin perjuicio de lo establecido en la disposición adicional primera.

Artículo 8. *Solicitud de publicación.*

1. La Dirección General de Tráfico habilitará un sistema que recibirá por medios electrónicos las solicitudes de publicación de los emisores autorizados, proporcionando las

garantías establecidas en el artículo 31 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Para el intercambio electrónico de información a través de este sistema con los organismos públicos emisores de edictos, se emplearán los sistemas de firma electrónica relacionados en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

2. A la solicitud, que deberá ser remitida con una antelación mínima de dos días hábiles a la fecha de publicación, se acompañará el texto del edicto en formato electrónico, de acuerdo con las garantías, especificaciones y modelos que se establezcan en el referido sistema informático.

3. Cuando el organismo emisor tenga su sede en el territorio de una Comunidad Autónoma con lengua cooficial propia, deberá enviar el edicto para su publicación en castellano y, además, podrá enviarlo en la lengua cooficial propia. En este caso, la publicación se hará en ambas lenguas. En caso de discrepancia prevalecerá el texto que determine el organismo emisor.

4. El organismo emisor que haya solicitado la publicación del edicto será el responsable de su contenido. La Dirección General de Tráfico mantendrá un registro de los organismos que envíen edictos para su publicación y en la sede electrónica del Organismo Autónomo Jefatura Central de Tráfico estará disponible un directorio actualizado de los mismos.

5. El intercambio de información y servicios entre el Tablón Edictal de Sanciones de Tráfico y los organismos emisores deberá realizarse preferentemente a través de la Red de comunicaciones de las Administraciones Públicas españolas, salvo imposibilidad técnica, de acuerdo con lo señalado por el artículo 13 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Artículo 9. *Publicación de los edictos.*

1. Los originales de los edictos remitidos para su publicación serán custodiados en los mismos términos en que estén redactados y autorizados, sin que puedan modificarse.

2. Por cada edicto que se reciba para su publicación en el Tablón Edictal de Sanciones de Tráfico se compondrá, a partir del original, un edicto único que contendrá todos los datos sin aplicar la lista de excluidos. En el caso de que el organismo emisor lo haya enviado, además de en castellano, en la lengua cooficial propia, se compondrá el edicto único en ambas lenguas.

Ambos documentos tendrán carácter reservado, serán generados y custodiados según lo establecido en el artículo 32 del Real Decreto 3/2010, de 8 de enero, y no podrá facilitarse información acerca de ellos, excepto al Defensor del Pueblo, al Ministerio Fiscal, a la Agencia Estatal de Administración Tributaria o a los órganos equivalentes de la Administración Autonómica o Local, a los Jueces y Tribunales, así como al organismo emisor.

3. La Dirección General de Tráfico pondrá a disposición de los organismos emisores los mecanismos necesarios para que puedan consultar, en todo momento, el estado en que se encuentran los edictos que hayan enviado para su publicación.

Asimismo, pondrá a disposición de los órganos de fiscalización y control mecanismos que les permitan acceder en cualquier momento al contenido de los edictos originales, así como verificar su origen y autenticidad.

4. La corrección de los errores existentes en los edictos publicados se podrá realizar a petición de quien hubiera solicitado la publicación y por el mismo procedimiento previsto para ésta, o de oficio por la Dirección General de Tráfico cuando sea resultado de algún error de composición, transcripción o grabación, siempre que suponga una alteración o modificación de su contenido de manera que pueda suscitar dudas.

5. La publicación de los edictos en el Tablón Edictal de Sanciones de Tráfico se efectuará sin contraprestación económica por parte de la Administración que la haya solicitado.

Artículo 10. *Plazo de publicación de los edictos.*

1. La Dirección General de Tráfico mantendrá expuesto el edicto en el Tablón Edictal de Sanciones de Tráfico en estado vigente, durante un plazo de veinte días naturales.

2. Si durante el plazo de publicación del edicto el Tablón Edictal de Sanciones de Tráfico estuviera inaccesible para los ciudadanos por cuestiones extraordinarias de carácter técnico del propio Tablón Edictal de Sanciones de Tráfico, dicho plazo se prorrogará automáticamente por un plazo igual al de los días que haya estado inaccesible. A estos efectos, sólo se considerará que el Tablón Edictal de Sanciones de Tráfico ha estado inaccesible si el problema técnico se ha mantenido durante días completos.

3. En especial, a los efectos del cómputo de los plazos que corresponda, se establecerá el mecanismo que garantice la constatación de la fecha y la hora de la publicación del edicto. La sincronización de la fecha y de la hora se realizará de acuerdo con lo previsto en el artículo 15 del Real Decreto 4/2010, de 8 de enero.

4. Finalizado el plazo de publicación o el período de vigencia, la notificación se tendrá por practicada y podrá continuarse el procedimiento. No obstante, el edicto seguirá estando accesible durante un año en el Tablón Edictal de Sanciones de Tráfico en estado no vigente. Una vez transcurrido este plazo, sólo tendrán acceso al mismo el propio interesado o su representante, el Defensor del Pueblo, el Ministerio Fiscal, la Agencia Estatal de Administración Tributaria o los órganos equivalentes de la Administración Autonómica o Local, y los Jueces y Tribunales.

Artículo 11. *Diligencia de acreditación de publicación.*

La Dirección General de Tráfico, una vez finalizado el plazo de publicación del edicto en el Tablón Edictal de Sanciones de Tráfico, enviará por medios electrónicos al organismo emisor, o pondrá a su disposición en la sede electrónica los mecanismos de carácter informático necesarios para obtenerla, una diligencia acreditativa de la publicación firmada electrónicamente, en la que figurarán los datos del edicto y las fechas en que ha permanecido expuesto en estado vigente.

Disposición adicional primera. *Interoperabilidad con los Tablones Edictales de las Comunidades Autónomas con competencias ejecutivas en materia de tráfico.*

En el supuesto de que las Comunidades Autónomas con competencias ejecutivas en materia de tráfico, de conformidad con lo dispuesto en la disposición adicional quinta de la Ley 18/2009, de 23 de noviembre, creen sus propios Tablones Edictales, en los cuales podrán efectuar las publicaciones de las notificaciones sancionadoras propias, así como las de las Administraciones Locales pertenecientes a sus ámbitos territoriales con las que hayan suscrito el correspondiente convenio de colaboración, estos Tablones y el Tablón Edictal de Sanciones de Tráfico deberán interoperar entre sí para permitir que el ciudadano, a través de un único acceso, pueda tener conocimiento de la publicación de cualquier notificación de un procedimiento sancionador que se esté tramitando contra él.

Disposición adicional segunda. *Protección de datos de carácter personal.*

1. El funcionamiento, la gestión y la publicación de edictos en el Tablón Edictal de Sanciones de Tráfico se realizará conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su reglamento de desarrollo, así como en el resto de la normativa que le sea de aplicación.

2. A los efectos de lo dispuesto en la mencionada normativa, la Dirección General de Tráfico, a la que corresponde la gestión del Tablón Edictal de Sanciones de Tráfico, tendrá la condición de responsable del fichero.

Las Administraciones con competencias ejecutivas en materia de tráfico, circulación de vehículos de motor y seguridad vial a las que se refiere el artículo 1.1 de esta orden distintas a la Dirección General de Tráfico tendrán, conforme a la citada normativa, la condición de responsables del tratamiento respecto de los datos correspondientes a los edictos cuya publicación en el Tablón Edictal de Sanciones de Tráfico, sea ordenada por aquéllas.

La Dirección General de Tráfico será igualmente responsable del tratamiento en relación con los edictos relacionados correspondientes a los procedimientos sancionadores cuya resolución sea competencia de los Jefes Provinciales y Locales de Tráfico.

3. Los responsables del tratamiento serán responsables del cumplimiento de los principios de protección de datos respecto de los edictos cuya publicación en el Tablón Edictal de Sanciones de Tráfico, ordenen.

En particular, en el ámbito de sus respectivas competencias corresponde a los responsables del tratamiento determinar el uso y contenido de los datos de carácter personal publicados en el Tablón Edictal de Sanciones de Tráfico, así como la posibilidad de su bloqueo cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubiera sido efectuada dicha publicación con anterioridad al plazo máximo de conservación de los edictos en el Tablón Edictal de Sanciones de Tráfico, al que se refiere el artículo10.4 de esta orden.

Disposición adicional tercera. *Accesibilidad.*

Sin perjuicio de lo dispuesto en esta orden se garantizará el acceso de los ciudadanos al conocimiento de los actos administrativos del procedimiento sancionador en materia de tráfico que les afecten, en los términos previstos en la normativa vigente al efecto.

Disposición transitoria única. *Publicación en el Tablón Edictal de Sanciones de Tráfico de las notificaciones por las Administraciones Locales.*

La implantación efectiva de la publicación en el Tablón Edictal de Sanciones de Tráfico de las notificaciones que no se hayan podido practicar en la Dirección Electrónica Vial o en el domicilio del interesado, por parte de las Administraciones Locales con competencia sancionadora en materia de tráfico, se podrá realizar de forma progresiva en función de la disponibilidad de los medios técnicos necesarios para ello.

En todo caso, éstas vendrán obligadas a efectuar la publicación en el Tablón Edictal de Sanciones de Tráfico de dichas notificaciones a partir del 25 de mayo de 2012.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente orden.

Disposición final primera. *Título competencial.*

La presente orden se dicta al amparo de lo dispuesto en el artículo 149.1.21.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de tráfico y circulación de vehículos a motor.

Disposición final segunda. *Habilitación normativa.*

Por Resolución del Director General de Tráfico publicada en el «Boletín Oficial del Estado» se informará de la fecha en que cada Administración Local se ha incorporado a la publicación de las notificaciones en el Tablón Edictal de Sanciones de Tráfico.

Disposición final tercera. *Modificación de la Orden INT/3764/2004, de 11 de noviembre, por la que se adecuan los ficheros informáticos del Ministerio del Interior que contienen datos de carácter personal a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y se crean nuevos ficheros cuya gestión corresponde a dicho Ministerio.*

En el apartado «Dirección General de Tráfico» del anexo I de la Orden INT/3764/2004, de 11 de noviembre, por la que se adecuan los ficheros informáticos del Ministerio del Interior que contienen datos de carácter personal a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y se crean nuevos ficheros cuya gestión corresponde a dicho Ministerio, se incluyen los siguientes ficheros:

1. 89 tris. Nombre del fichero: Tablón Edictal de Sanciones de Tráfico.

a) Finalidad del fichero: Gestionar el Tablón Edictal de Sanciones de Tráfico.

b) Usos previstos: Gestión administrativa de la publicación a través de edictos de las notificaciones a que dé lugar el procedimiento sancionador como consecuencia de la comisión de infracciones a la normativa sobre tráfico, circulación de vehículos a motor y

seguridad vial, que no se hayan podido practicar en la Dirección Electrónica Vial o en el domicilio del interesado, con independencia de cuál sea la autoridad sancionadora competente.

c) Personas o colectivos de los que se obtienen los datos o que resulten obligados a suministrarlos: Organismos emisores autorizados para solicitar la publicación a través de edictos en el Tablón Edictal de Sanciones de Tráfico de las notificaciones que no se hayan podido practicar en la Dirección Electrónica Vial o en el domicilio del interesado.

d) Procedimiento de recogida de los datos: Aplicaciones informáticas establecidas al efecto.

e) Estructura básica del fichero y descripción de los datos recogidos: Contiene datos de los organismos emisores autorizados para solicitar la publicación a través de edictos de las notificaciones: nombre, apellidos, DNI o NIE, clave pública de la firma electrónica; así como los datos de las personas a las que se notifica mediante los edictos: nombre, apellidos o denominación social, DNI, NIE o CIF.

f) Sistema de tratamiento: Automatizado.

g) Cesiones de datos previstas: Defensor del Pueblo, Ministerio Fiscal, Agencia Estatal de Administración Tributaria, Jueces y Tribunales.

h) Transferencias internacionales previstas a terceros países: No se prevén.

i) Órgano responsable del fichero: Dirección General de Tráfico.

j) Órgano ante el que pueden ejercitarse los derechos de rectificación, cancelación y oposición: Dirección General de Tráfico,calle Josefa Valcárcel 44, 28071 Madrid.

k) Medidas de seguridad: Nivel medio.

2. 89 quáter. Nombre del fichero: Lista de excluidos del Tablón Edictal de Sanciones de Tráfico.

a) Finalidad del fichero: Gestionar el servicio «lista de excluidos» del Tablón Edictal de Sanciones de Tráfico.

b) Usos previstos: Gestión administrativa de los datos personales de quienes soliciten el alta o la baja en el servicio «lista de excluidos» para impedir que puedan ser visualizados por cualquier persona que acceda a los edictos publicados en el Tablón Edictal de Sanciones de Tráfico.

c) Personas o colectivos de los que se obtienen los datos o que resulten obligados a suministrarlos: Aquellas que soliciten el alta o la baja en el servicio «lista de excluidos» para que sus datos personales contenidos en los edictos publicados en el Tablón Edictal de Sanciones de Tráfico no puedan ser visualizados más que por ellos mismos y por las personas a las cuáles haya autorizado.

d) Procedimiento de recogida de los datos: Aplicaciones informáticas establecidas al efecto.

e) Estructura básica del fichero y descripción de los datos recogidos: Contiene datos de las personas que han solicitado el alta en el servicio «lista de excluidos»: nombre, apellidos, DNI o NIE, domicilio, clave pública de la firma electrónica.

f) Sistema de tratamiento: Automatizado.

g) Cesiones de datos previstas: Ninguna.

h) Transferencias internacionales previstas a terceros países: No se prevén.

i) Órgano responsable del fichero: Dirección General de Tráfico.

j) Órgano ante el que pueden ejercitarse los derechos de rectificación, cancelación y oposición: Dirección General de Tráfico, calleJosefa Valcárcel, 44, 28071 Madrid.

k) Medidas de seguridad: Nivel medio.

Disposición final cuarta. *Entrada en vigor.*

La presente orden entrará en vigor el mismo día de su publicación en el «Boletín Oficial del Estado».