Códigos electrónicos

Código de Administración Electrónica

Selección y ordenación:
Joaquín Meseguer Yebra

Edición actualizada a 10 de febrero de 2014

BOLETÍN OFICIAL DEL ESTADO

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

Alertas de actualización en BOE a la Carta: www.boe.es/a_la_carta/

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

© Agencia Estatal Boletín Oficial del Estado

NIPO: 007-13-037-X

Catálogo de Publicaciones de la Administración General del Estado
publicacionesoficiales.boe.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
tel. 911 114 000 – www.boe.es

SUMARIO

§ 1. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. . . . 1

§ 2. 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 30

§ 3. 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 58

§ 4. 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 106

REGISTROS ELECTRÓNICOS

§ 5. Orden HAP/566/2013, de 8 de abril, por la que se regula el Registro Electrónico Común. 124

§ 6. Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos 132

BOLETÍN OFICIAL DEL ESTADO

§ 7. Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado» 144

§ 8. Orden 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». 153

SISTEMAS DE VERIFICACIÓN DE DATOS

§ 9. Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad 156

§ 10. Orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia 161

FIRMA ELECTRÓNICA

§ 11. Ley 59/2003, de 19 de diciembre, de firma electrónica 166

§ 12. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica 191

NOTIFICACIÓN ELECTRÓNICA

§ 13. Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre. . 198

CONTRATACIÓN ADMINISTRATIVA

§ 14. Orden EHA/1307/2005, de 29 de abril, por la que se regula el empleo de medios electrónicos en los procedimientos de contratación 203

§ 15. Orden EHA/1220/2008, de 30 de abril, por la que se aprueban las instrucciones para operar en la Plataforma de Contratación del Estado. 210

SEGURIDAD SOCIAL

§ 16. Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social 219

COMUNICACIÓN DIGITAL

§ 17. Resolución de 21 de marzo de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Guía de Comunicación Digital para la Administración General del Estado. . . . 228

ÍNDICE SISTEMÁTICO

§ 1. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos . . . 1

Preámbulo . . . 1
TÍTULO PRELIMINAR. Del ámbito de aplicación y los principios generales . . . 8
TÍTULO PRIMERO. Derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos . . . 10
TÍTULO SEGUNDO. Régimen jurídico de la administración electrónica . . . 13
CAPÍTULO I. De la sede electrónica . . . 13
CAPÍTULO II. De la identificación y autenticación . . . 13
Sección 1.ª Disposiciones comunes . . . 13
Sección 2.ª Identificación de los ciudadanos y autenticación de su actuación . . . 14
Sección 3.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia . . . 15
Sección 4.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos . . . 16
CAPÍTULO III. De los registros, las comunicaciones y las notificaciones electrónicas . . . 17
Sección 1.ª De los Registros . . . 17
Sección 2.ª De las comunicaciones y las notificaciones electrónicas . . . 18
CAPÍTULO IV. De los documentos y los archivos electrónicos . . . 19
TÍTULO TERCERO. De la gestión electrónica de los procedimientos . . . 20
CAPÍTULO I. Disposiciones comunes . . . 20
CAPÍTULO II. Utilización de medios electrónicos en la tramitación del procedimiento . . . 21
TÍTULO CUARTO. Cooperación entre administraciones para el impulso de la administración electrónica . . . 22
CAPÍTULO I. Marco institucional de cooperación en materia de administración electrónica . . . 22
CAPÍTULO II. Cooperación en materia de interoperabilidad de sistemas y aplicaciones . . . 23
CAPÍTULO III. Reutilización de aplicaciones y transferencia de tecnologías . . . 24
Disposiciones adicionales . . . 24
Disposiciones transitorias . . . 25
Disposiciones derogatorias . . . 25
Disposiciones finales . . . 26
ANEXO. Definiciones . . . 28

§ 2. 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 . . . 30

Preámbulo . . . 30
TÍTULO I. Disposiciones generales . . . 33
TÍTULO II. Sedes electrónicas y punto de acceso general a la Administración General del Estado . . . 34
TÍTULO III. Identificación y autenticación . . . 37
CAPÍTULO I. Identificación y autenticación en el acceso electrónico de los ciudadanos a la Administración General del Estado y sus organismos públicos vinculados o dependientes . . . 37
CAPÍTULO II. Identificación y autenticación de sedes electrónicas y de las comunicaciones que realicen los órganos de la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla . . . 40
CAPÍTULO III. Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad . . . 42
TÍTULO IV. Registros electrónicos . . . 44
TÍTULO V. De las comunicaciones y las notificaciones . . . 46
CAPÍTULO I. Comunicaciones electrónicas . . . 46
CAPÍTULO II. Notificaciones electrónicas . . . 47
TÍTULO VI. Los documentos electrónicos y sus copias . . . 49
CAPÍTULO I. Disposiciones comunes sobre los documentos electrónicos . . . 49
CAPÍTULO II. Normas específicas relativas a los documentos administrativos electrónicos . . . 52

CAPÍTULO III. Normas específicas relativas a los documentos electrónicos aportados por los ciudadanos . . . 52
CAPÍTULO IV. Normas relativas a la obtención de copias electrónicas por los ciudadanos . . . 53
CAPÍTULO V. Archivo electrónico de documentos . . . 53
CAPÍTULO VI. Expediente electrónico . . . 54
Disposiciones adicionales . . . 54
Disposiciones transitorias . . . 55
Disposiciones derogatorias . . . 56
Disposiciones finales . . . 56

§ 3. 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 . . . 58

Preámbulo . . . 58
CAPÍTULO I. Disposiciones generales . . . 60
CAPÍTULO II. Principios básicos . . . 61
CAPÍTULO III. Requisitos mínimos . . . 62
CAPÍTULO IV. Comunicaciones electrónicas . . . 66
CAPÍTULO V. Auditoría de la seguridad . . . 67
CAPITULO VI. Estado de seguridad de los sistemas . . . 68
CAPÍTULO VII. Respuesta a incidentes de seguridad . . . 68
CAPÍTULO VIII. Normas de conformidad . . . 69
CAPÍTULO IX. Actualización . . . 69
CAPÍTULO X. Categorización de los sistemas de información . . . 69
Disposiciones adicionales . . . 70
Disposiciones transitorias . . . 70
Disposiciones derogatorias . . . 71
Disposiciones finales . . . 71
ANEXOS . . . 71
ANEXO I. Categorías de los sistemas . . . 71
ANEXO II. Medidas de seguridad . . . 73
ANEXO III. Auditoría de la seguridad . . . 103
ANEXO IV. Glosario . . . 104
ANEXO V. Modelo de cláusula administrativa particular . . . 105

§ 4. 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 . . . 106

Preámbulo . . . 106
CAPÍTULO I. Disposiciones generales . . . 108
CAPÍTULO II. Principios básicos . . . 109
CAPÍTULO III. Interoperabilidad organizativa . . . 109
CAPÍTULO IV. Interoperabilidad semántica . . . 110
CAPÍTULO V. Interoperabilidad técnica . . . 111
CAPÍTULO VI. Infraestructuras y servicios comunes . . . 112
CAPÍTULO VII. Comunicaciones de las Administraciones públicas . . . 112
CAPÍTULO VIII. Reutilización y transferencia de tecnología . . . 112
CAPÍTULO IX. Firma electrónica y certificados . . . 113
CAPÍTULO X. Recuperación y conservación del documento electrónico . . . 115
CAPÍTULO XI. Normas de conformidad . . . 117
CAPÍTULO XII. Actualización . . . 118
Disposiciones adicionales . . . 118
Disposiciones transitorias . . . 119
Disposiciones derogatorias . . . 120
Disposiciones finales . . . 120
ANEXO. Glosario de términos . . . 120

REGISTROS ELECTRÓNICOS

§ 5. Orden HAP/566/2013, de 8 de abril, por la que se regula el Registro Electrónico Común . . . 124

Preámbulo . . . 124
Artículos . . . 125
Disposiciones adicionales . . . 129
Disposiciones transitorias . . . 129

Disposiciones derogatorias . . . 129
Disposiciones finales . . . 129
ANEXO I. Formulario de propósito general . . . 129
ANEXO II. Formulario de inscripción a pruebas selectivas . . . 130
ANEXO III. Fichero de datos personales . . . 131

§ 6. Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos . . . 132

Preámbulo . . . 132
Artículos . . . 133
Disposiciones adicionales . . . 138
Disposiciones finales . . . 138
ANEXO I . . . 139
ANEXO II . . . 141
ANEXO III . . . 143
ANEXO IV . . . 143

BOLETÍN OFICIAL DEL ESTADO

§ 7. Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado» . . . 144

Preámbulo . . . 144
CAPÍTULO I. Disposiciones generales . . . 145
CAPÍTULO II. Contenido del «Boletín Oficial del Estado» . . . 146
CAPÍTULO III. Edición electrónica . . . 147
CAPÍTULO IV. Acceso de los ciudadanos al «Boletín Oficial del Estado» . . . 148
CAPÍTULO V. Procedimiento de publicación . . . 149
Disposiciones transitorias . . . 151
Disposiciones derogatorias . . . 152
Disposiciones finales . . . 152

§ 8. Orden 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» . . . 153

Preámbulo . . . 153
Artículos . . . 154
ANEXO. Características de la aplicación informática «Insértese digital» . . . 155

SISTEMAS DE VERIFICACIÓN DE DATOS

§ 9. Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad . . . 156

Preámbulo . . . 156
Artículos . . . 157
Disposiciones finales . . . 157
ANEXO. Reglamento Técnico del Sistema de Verificación de Datos de Identidad . . . 158

§ 10. Orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia . . . 161

Preámbulo . . . 161
Artículos . . . 162
Disposiciones finales . . . 162
ANEXO. Reglamento Técnico del Sistema de Verificación de Datos de Residencia . . . 162

FIRMA ELECTRÓNICA

§ 11. Ley 59/2003, de 19 de diciembre, de firma electrónica 166

Preámbulo 166
TÍTULO I. Disposiciones generales 170
TÍTULO II. Certificados electrónicos 173
CAPÍTULO I. Disposiciones generales 173
CAPÍTULO II. Certificados reconocidos 175
CAPÍTULO III. El documento nacional de identidad electrónico 177
TÍTULO III. Prestación de servicios de certificación 177
CAPÍTULO I. Obligaciones 177
CAPÍTULO II. Responsabilidad 180
TÍTULO IV. Dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica 181
CAPÍTULO I. Dispositivos de firma electrónica 181
CAPÍTULO II. Certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica 182
TÍTULO V. Supervisión y control 183
TÍTULO VI. Infracciones y sanciones 184
Disposiciones adicionales 186
Disposiciones transitorias 190
Disposiciones derogatorias 190
Disposiciones finales 190

§ 12. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica 191

Preámbulo 191
Artículos 192
Disposiciones adicionales 196
Disposiciones transitorias 197
Disposiciones derogatorias 197
Disposiciones finales 197

NOTIFICACIÓN ELECTRÓNICA

§ 13. Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre 198

Preámbulo 198
Artículos 199
Disposiciones transitorias 202
Disposiciones derogatorias 202
Disposiciones finales 202

CONTRATACIÓN ADMINISTRATIVA

§ 14. Orden EHA/1307/2005, de 29 de abril, por la que se regula el empleo de medios electrónicos en los procedimientos de contratación 203

Preámbulo 203
Artículos 204
ANEXO. Formatos admisibles para los documentos intercambia-dos en los procesos de contratación electrónica 209

§ 15. Orden EHA/1220/2008, de 30 de abril, por la que se aprueban las instrucciones para operar en la Plataforma de Contratación del Estado 210

Preámbulo 210
CAPÍTULO I. Disposiciones Generales 211
CAPÍTULO II. Publicación del Perfil de Contratante en la Plataforma de Contratación del Estado 211
CAPÍTULO III. Publicación de información por órganos con competencias consultivas o de ordenación en materia de contratación pública 214
Disposiciones finales 214
ANEXO I. Datos para el alta del perfil del contratante 214
ANEXO II. Alta de un usuario 215
ANEXO III. Especificaciones de contenidos y formatos correspondientes a la arquitectura de información CODICE 215
ANEXO IV. Especificaciones de los protocolos de comunicación de información 217

SEGURIDAD SOCIAL

§ 16. Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social 219

Preámbulo 219
Artículos 220
Disposiciones adicionales 225
Disposiciones transitorias 226
Disposiciones derogatorias 226
Disposiciones finales 226

COMUNICACIÓN DIGITAL

§ 17. Resolución de 21 de marzo de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Guía de Comunicación Digital para la Administración General del Estado 228

Preámbulo 228
Artículos 229

§ 1

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

Jefatura del Estado
«BOE» núm. 150, de 23 de junio de 2007
Última modificación: 5 de marzo de 2011
Referencia: BOE-A-2007-12352

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presenten vieren y entedieren.

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

EXPOSICIÓN DE MOTIVOS

I

Determinadas edades de la humanidad han recibido su denominación de las técnicas que se empleaban en las mismas y hoy podríamos decir que las tecnologías de la información y las comunicaciones están afectando también muy profundamente a la forma e incluso al contenido de las relaciones de los seres humanos entre sí y de las sociedades en que se integran. El tiempo actual –y en todo caso el siglo XXI, junto con los años finales del XX–, tiene como uno de sus rasgos característicos la revolución que han supuesto las comunicaciones electrónicas. En esa perspectiva, una Administración a la altura de los tiempos en que actúa tiene que acompañar y promover en beneficio de los ciudadanos el uso de las comunicaciones electrónicas. Estos han de ser los primeros y principales beneficiarios del salto, impensable hace sólo unas décadas, que se ha producido en el campo de la tecnología de la información y las comunicaciones electrónicas. Al servicio, pues, del ciudadano la Administración queda obligada a transformarse en una administración electrónica regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución.

Es en ese contexto en el que las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades que la sociedad de la información tiene, asumiendo su responsabilidad de contribuir a hacer realidad la sociedad de la información. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las Administraciones Públicas. Depende de la confianza y seguridad que genere en los ciudadanos y depende también de los servicios que ofrezca.

El mejor servicio al ciudadano constituye la razón de la reformas que tras la aprobación de la Constitución se han ido realizando en España para configurar una Administración moderna que haga del principio de eficacia y eficiencia su eje vertebrador siempre con la mira puesta en los ciudadanos. Ese servicio constituye también la principal razón de ser de la Ley de acceso electrónico de los ciudadanos a los servicios públicos que trata, además, de estar a la altura de la época actual.

En efecto, la descentralización política del Estado no se agotó en su primer y más inmediato designio de organizar políticamente España de una forma muy diferente al Estado unitario, sino que ha sido ocasión para que la mayor proximidad democrática de los nuevos poderes autonómicos se tradujese también en una mayor proximidad de las Administraciones de ellos dependientes respecto del ciudadano.

En la misma línea se mueve el reconocimiento constitucional de la autonomía local.

No obstante, esa mayor proximidad al ciudadano de la Administración, derivada de la descentralización autonómica y local, no ha acabado de superar la barrera que sigue distanciando todavía al ciudadano de la Administración, de cualquier Administración, incluida la del Estado, y que, muchas veces, no es otra que la barrera que levanta el tiempo y el espacio: el tiempo que hay que dedicar a la relación con aquélla para la realización de muchos trámites de la vida diaria que empiezan a veces por la necesidad de una primera información que exige un desplazamiento inicial, más los sucesivos desplazamientos y tiempo que se dedican a posteriores trámites a hacer con la Administración para las actividades más elementales. Esas primeras barreras potencian, en ocasiones, otras que afectan a la posición servicial de las Administraciones Públicas. Éstas no pueden cumplir siempre su misión atendiendo cualquier cosa que pida un ciudadano, puesto que puede estar en contradicción con los intereses de la mayoría de los demás ciudadanos, con los intereses generales representados por las leyes. Pero en esos casos –en que los intereses generales no coinciden con los intereses individuales– la relación con el ciudadano debe ser, también, lo más rápida y clara posible sin pérdidas de tiempo innecesarias.

En todo caso, esas primeras barreras en las relaciones con la Administración –la distancia a la que hay que desplazarse y el tiempo que es preciso dedicar– hoy día no tienen razón de ser. Las tecnologías de la información y las comunicaciones hacen posible acercar la Administración hasta la sala de estar de los ciudadanos o hasta las oficinas y despachos de las empresas y profesionales. Les permiten relacionarse con ella sin colas ni esperas. E incluso recibir servicios e informaciones ajenos a actividades de intervención administrativa o autorización; informaciones y servicios no relacionados con actuaciones limitadoras, sino al contrario ampliadoras de sus posibilidades. Esas condiciones permiten también a los ciudadanos ver a la Administración como una entidad a su servicio y no como una burocracia pesada que empieza por exigir, siempre y para empezar, el sacrificio del tiempo y del desplazamiento que impone el espacio que separa el domicilio de los ciudadanos y empresas de las oficinas públicas. Pero, además de eso, las nuevas tecnologías de la información facilitan, sobre todo, el acceso a los servicios públicos a aquellas personas que antes tenían grandes dificultades para llegar a las oficinas públicas, por motivos de localización geográfica, de condiciones físicas de movilidad u otros condicionantes, y que ahora se pueden superar por el empleo de las nuevas tecnologías. Se da así un paso trascendental para facilitar, en igualdad de condiciones, la plena integración de estas personas en la vida pública, social, laboral y cultural.

De ello se percató la Ley 30/1992 de 26 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC), que en su primera versión recogió ya en su artículo 45 el impulso al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, por parte de la Administración al objeto de desarrollar su actividad y el ejercicio de sus competencias y de permitir a los ciudadanos relacionarse con las Administraciones cuando fuese compatible con los «medios técnicos de que dispongan».

Esa previsión, junto con la de la informatización de registros y archivos del artículo 38 de la misma Ley en su versión originaria y, especialmente, en la redacción que le dio la Ley 24/2001 de 27 de diciembre al permitir el establecimiento de registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones por medios telemáticos, abría el paso a la utilización de tales medios para relacionarse con la Administración.

Simultáneamente, la misma Ley 24/2001 modificó el artículo 59 permitiendo la notificación por medios telemáticos si el interesado hubiera señalado dicho medio como preferente o consentido expresamente.

En el mismo sentido destacan las modificaciones realizadas en la Ley General Tributaria para permitir también las notificaciones telemáticas así como el artículo 96 de la nueva Ley General Tributaria de 2003 que prevé expresamente la actuación administrativa automatizada o la imagen electrónica de los documentos.

Sin embargo, el desarrollo de la administración electrónica es todavía insuficiente. La causa en buena medida se debe a que las previsiones de los artículos 38, 45 y 59 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común son facultativas. Es decir, dejan en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo, o no, relacionarse por medios electrónicos con ellas, según que éstas quieran poner en pie los instrumentos necesarios para esa comunicación con la Administración.

Por ello esta Ley pretende dar el paso del «podrán» por el «deberán».

Las avanzadas para el momento, pero por otra parte prudentes, previsiones legales, muy válidas en 1992 o en 2001, hoy han quedado desfasadas, ante una realidad en que el grado de penetración de ordenadores y el número de personas y entidades con acceso en banda ancha a Internet, con las posibilidades abiertas a otras tecnologías y plataformas, no se corresponden ya con los servicios meramente facultativos que la Ley citada permite y estimula a establecer a las Administraciones.

El servicio al ciudadano exige consagrar su derecho a comunicarse con las Administraciones por medios electrónicos. La contrapartida de ese derecho es la obligación de éstas de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse. Esa es una de las grandes novedades de la Ley: pasar de la declaración de impulso de los medios electrónicos e informáticos –que se concretan en la práctica en la simple posibilidad de que algunas Administraciones, o algunos de sus órganos, permitan las comunicaciones por medios electrónicos– a que estén obligadas a hacerlo porque la Ley reconoce el derecho de los ciudadanos a establecer relaciones electrónicas.

La Ley consagra la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones. El reconocimiento de tal derecho y su correspondiente obligación se erigen así en el eje central del proyecto de Ley.

Pero en torno a dicho eje es preciso abordar muchas otras que contribuyen a definir y concretar el alcance de ese derecho. Así, por ejemplo, tal derecho se hace efectivo de modo real mediante la imposición, al menos en el ámbito de la Administración General del Estado y en los términos de la ley, de la obligación de poner a disposición de ciudadanos y empresas al menos un punto de acceso general a través del cual los usuarios puedan, de forma sencilla, acceder a la información y servicios de su competencia; presentar solicitudes y recursos; realizar el trámite de audiencia cuando proceda; efectuar pagos o acceder a las notificaciones y comunicaciones que les remitan la Administración Pública.

También debe encontrar información en dicho punto de acceso único sobre los servicios multicanal o que le sean ofrecidos por más de un medio, tecnología o plataforma.

II

La Ley se articula a partir de las competencias del Estado que le reconoce el artículo 149.1.18 de la Constitución: «Bases del régimen jurídico de las Administraciones Públicas», por una parte y «procedimiento administrativo común» por otra.

Por otra parte, la regulación estatal, en lo que tiene de básico, deja margen a los desarrollos autonómicos, sin que pueda olvidarse, además, que el objeto de las bases en este caso deben permitir «en todo caso», de acuerdo con este número 18, un «tratamiento común» ante ellas.

En esta perspectiva, la regulación del Estado debe abordar aquellos aspectos en los que es obligado que las previsiones normativas sean comunes, como es el caso de la interoperabilidad, las garantías de las comunicaciones electrónicas, los servicios a los que tienen derecho los ciudadanos, la conservación de las comunicaciones electrónicas y los demás temas que se abordan en la ley para garantizar que el ejercicio del derecho a

relacionarse electrónicamente con todas las administraciones forme parte de ese tratamiento común que tienen.

La Ley 30/1992 se limitó a abrir la posibilidad, como se ha dicho, de establecer relaciones telemáticas con las Administración, pero la hora actual demanda otra regulación que garantice, pero ahora de modo efectivo, un tratamiento común de los ciudadanos antes todas las Administraciones: que garantice, para empezar y sobre todo, el derecho a establecer relaciones electrónicas con todas las Administraciones Públicas. Las nuevas realidades, exigencias y experiencias que se han ido poniendo de manifiesto; el propio desarrollo de la sociedad de la información, la importancia que una regulación clara, precisa y común de los derechos de los ciudadanos y el cambio de circunstancias tecnológicas y sociales exige actualizar el contenido, muy diferente al de 1992, de la regulación básica que esté hoy a la altura de las nueva exigencias. Esa regulación común exige, hoy, por ejemplo, reconocer el derecho de los ciudadanos –y no sólo la posibilidad– de acceder mediante comunicaciones electrónicas a la Administración.

III

El reconocimiento general del derecho de acceder electrónicamente a las Administraciones Públicas tiene otras muchas consecuencias a las que hay dar solución y de las que aquí, de forma resumida, se enumeran algunas.

Así, en primer lugar, la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de unos datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo expediente en el que es evidente, desde luego, pero, sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente. Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal deben bastar, y no se trata de hacer ninguna innovación al respecto, pero sí de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración.

Por otra parte, los interesados en un procedimiento tienen derecho de acceso al mismo y ver los documentos. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe poder permitir el acceso en línea a los interesados para verificar la situación del expediente, sin mengua de todas las garantías de la privacidad.

En todo caso, la progresiva utilización de comunicaciones electrónicas, derivada del reconocimiento del derecho a comunicarse electrónicamente con la Administración, suscita la cuestión no ya de la adaptación de ésta –recursos humanos y materiales– a una nueva forma de relacionarse con los ciudadanos, sino también la cuestión de la manera de adaptar sus formas de actuación y tramitación de los expedientes y en general adaptar los procedimientos a la nueva realidad que imponen las nuevas tecnologías.

El hecho de reconocer el derecho de los ciudadanos a comunicarse electrónicamente con la Administración plantea, en primer lugar, la necesidad de definir claramente la «sede» administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad. Exige también abordar la definición a los efectos de la Ley de una serie de términos y conceptos cuyo uso habitual obliga en un contexto de comunicaciones electrónicas a efectuar muchas precisiones. Tal sucede con la definición de expediente electrónico y de documento electrónico; de los registros electrónicos y de las notificaciones electrónicas o del alcance y sistemas de sellados de tiempo.

La consagración de ese derecho de los ciudadanos a comunicarse electrónicamente con la Administración suscita, también, por ejemplo, la cuestión de la forma de utilizar y archivar dichas comunicaciones. Y lo plantea tanto en lo que podría considerarse la formación del expediente o el archivo de oficina –el vinculado a la tramitación de los expedientes–, como en lo que se refiere al archivo de los expedientes ya tramitados.

En cuanto al funcionamiento interno de la Administración, las nuevas tecnologías permiten oportunidades de mejora (eficiencia y reducción de costes) que hacen ineludible la consideración de las formas de tramitación electrónica, tanto para la tramitación electrónica

de expedientes, como para cualquier otra actuación interna de la Administración, expandiéndolas gradualmente con el objetivo del año 2009.

Ciertamente, el uso de medios electrónicos no puede significar merma alguna del derecho del interesado en un expediente a acceder al mismo en la forma tradicional, así como tampoco puede suponer un freno o un retraso para que la Administración internamente adopte los mecanismos más adecuados, en este caso medios electrónicos, que le permitan mejorar procesos y reducir el gasto público. Conjugar ambos requerimientos es posible gracias a las medidas de la política de fomento de desarrollo de la Sociedad de la Información que se vienen impulsando en los últimos años. En este sentido la Administración debe incorporar las nuevas tecnologías a su funcionamiento interno y, simultáneamente, se debe garantizar que aquellos ciudadanos que por cualquier motivo (no disponibilidad de acceso a las nuevas tecnologías o falta de formación) no puedan acceder electrónicamente a la Administración Pública, dispongan de los medios adecuados para seguir comunicándose con la Administración con los mismos derechos y garantías. La solución a ese doble objetivo pasa por la formación del personal al servicio de la Administración que atiende al público para que hagan posible la comunicación de estos ciudadanos con la administración electrónica, así como por la disponibilidad de puntos de acceso electrónico públicos en sedes administrativas. O también, desde luego, establecer las previsiones generales que sean garantía de los derechos de los ciudadanos y de un tratamiento igual ante todas las Administraciones en todos esos supuestos.

En segundo lugar es necesario regular la validez de los documentos y sus copias y la forma de que el documento electrónico opere con plena validez en modo convencional y, en su caso, la forma en que los documentos convencionales se transformen en documentos electrónicos.

Otra cuestión que se aborda es la de las plataformas que pueden utilizar los ciudadanos o las propias Administraciones para establecer tales comunicaciones electrónicas. El ordenador e Internet puede ser una vía, pero no es desde luego la única; las comunicaciones vía SMS pueden ser otra forma de actuación que en algunas Administraciones están siendo ya utilizadas. La Televisión Digital Terrestre, por ejemplo, abre también posibilidades con las que hay también que contar. La Ley no puede limitarse a regular el uso de los canales electrónicos disponibles hoy en día, ya que la gran velocidad en el desarrollo de las tecnologías de la información hacen posible la aparición de nuevos instrumentos electrónicos que pudieran aplicarse para la administración electrónica en muy poco tiempo, siendo necesario generalizar la regulación de estos canales.

La Ley debe partir del principio de libertad de los ciudadanos en la elección de la vía o canal por el que quieren comunicarse con la Administración, si bien cada tecnología puede ser apta para una función en razón de sus características y de la fiabilidad y seguridad de sus comunicaciones.

IV

Debe recordarse que el impulso de una administración electrónica supone también dar respuesta a los compromisos comunitarios y a las iniciativas europeas puestas en marcha a partir de Consejo Europeo de Lisboa y Santa Maria da Feira, continuado con sucesivas actuaciones hasta la actual comunicación de la Comisión «i2010: Una Sociedad de la Información Europea para el crecimiento y el empleo».

El impulso comunitario a la iniciativa e-Europa da la máxima importancia al desarrollo de la administración electrónica, buscando aprovechar todas las posibilidades de las nuevas tecnologías como un factor determinante del futuro económico de Europa.

En estos años de vigencia de la iniciativa e-Europa el ámbito de actuación de la administración electrónica ha crecido considerablemente en sucesivas revisiones, hasta llegar a noviembre de 2005, cuando, tras la publicación de la comunicación relativa a i2010 se aprobó, en la Cumbre de Manchester, una resolución ministerial, con objetivos concretos para el desarrollo de la administración electrónica en la Unión. Tras esta resolución se aprobó el Plan de Acción sobre administración electrónica i2010, en la que se señala que los éxitos de la administración electrónica son ya claramente visibles en varios países de la UE, estimando en 50.000 millones de euros el ahorro anual en toda la Unión que una implantación generalizada de ella podría generar.

Asimismo, el 12 de diciembre de 2006, y con objeto de avanzar en la consecución del objetivo fijado por el Consejo Europeo de Lisboa, se aprobó la Directiva 2006/123/CE, relativa a los servicios en el mercado interior.

Esta Directiva establece, entre otras obligaciones para los Estados miembros, la de facilitar por medios electrónicos acceso a los trámites relacionados con las actividades de servicios y a la información de interés tanto para los prestadores como para los destinatarios de los mismos.

Por ello, y dada la analogía de esta finalidad con el objetivo de esta Ley, se realiza en la misma una referencia expresa a la información y trámites relacionados con las actividades de servicios, de forma que los artículos 6, 7 y 8 de la Directiva pueden considerarse traspuestos por esta Ley.

Por otra parte, en el contexto internacional, también otros organismos se han interesado en la administración electrónica como forma de activar la economía y mejorar el gobierno de los países como es el caso de la OCDE, que publicó en 2004 un estudio con un título casi autodescriptivo: «La administración electrónica: Un imperativo», donde resalta los ahorros que la administración electrónica puede generar al permitirles aumentar su eficacia.

También el Consejo de Europa, desde una perspectiva más social, está analizando la administración electrónica como un motor de desarrollo. En diciembre de 2004 el Comité de Ministros adoptó una recomendación donde se señala que la administración electrónica no es asunto meramente técnico, sino de gobernanza democrática.

V

En este contexto, una Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas se justifica en la creación de un marco jurídico que facilite la extensión y utilización de estas tecnologías. Y el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías.

Por otro lado, la legislación debe proclamar y erigirse sobre un principio fundamental como es la conservación de las garantías constitucionales y legales a los derechos de los ciudadanos y en general de las personas que se relacionan con la Administración Pública, cuya exigencia se deriva del artículo 18.4 CE, al encomendar a la ley la limitación del uso de la informática para preservar el ejercicio de los derechos constitucionales. Esta conservación exige afirmar la vigencia de los derechos fundamentales no sólo como límite, sino como vector que orienta esta reforma legislativa de acuerdo con el fin promocional consagrado en el artículo 9.2 de nuestro texto fundamental, así como recoger aquellas peculiaridades que exigen la aplicación segura de estas tecnologías. Estos derechos deben completarse con otros exigidos por el nuevo soporte electrónico de relaciones, entre los que debe estar el derecho al uso efectivo de estos medios para el desarrollo de las relaciones de las personas con la Administración. Las anteriores consideraciones cristalizan en un Estatuto del ciudadano frente a la administración electrónica que recoge un elenco no limitativo de las posiciones del ciudadano en sus relaciones con las Administraciones Públicas, así como las garantías específicas para su efectividad.

Con este fin, la Ley crea la figura del Defensor del Usuario, que atenderá las quejas y realizará las sugerencias y propuestas pertinentes para mejorar las relaciones de ciudadanos en su trato con las Administraciones Públicas por medios electrónicos.

De otro lado, merece subrayarse el papel de vanguardia que corresponde a nuestras empresas en el desarrollo de una verdadera sociedad de la información y, por ende, de una Administración accesible electrónicamente. No en vano, la integración de las Tecnologías de la Información y las Comunicaciones (TIC's) en el día a día de la empresa, necesaria en virtud de las exigencias del entorno abierto y altamente competitivo en que operan, ha sido y es palanca impulsora para el desarrollo y creciente incorporación de esas mismas tecnologías en el actuar administrativo. Al mismo tiempo, representa una ayuda insustituible para favorecer la expansión de la «cultura electrónica» entre los trabajadores-ciudadanos.

Las empresas pueden, en tal sentido, desempeñar un papel coadyuvante clave para la consecución de los objetivos pretendidos por esta Ley. Las razones apuntadas aconsejan un tratamiento específico de aquellos procedimientos y gestiones que de forma más intensa afectan al desarrollo de la actividad empresarial.

A todo ello se debe la aprobación de esta Ley de acceso electrónico de los ciudadanos a los servicios públicos, en la que se incluyen las siguientes materias con la estructura que se recoge en los siguientes apartados.

VI

La Ley se estructura en cinco títulos, seis disposiciones adicionales, una disposición transitoria, una derogatoria y ocho finales.

En el Título Preliminar se definen el objeto y finalidades de la ley, los principios generales a los que se ajusta, así como su ámbito de aplicación. Debe destacarse el carácter básico de la ley en los términos establecidos en la disposición final primera, siendo por tanto de aplicación a todas las Administraciones Públicas los artículos referidos en dicha disposición final.

La Ley establece entre otros, el principio de igualdad, para que la utilización de comunicaciones electrónicas con las Administraciones Públicas no implique una discriminación para los ciudadanos que se relacionen con la Administración por medios no electrónicos.

En el Título Primero están recogidos los derechos de los ciudadanos en sus relaciones con las Administraciones Públicas a través de medios electrónicos. Para garantizar el pleno ejercicio de estos derechos, se establece la obligación de las Administraciones de habilitar diferentes canales o medios para la prestación de los servicios electrónicos.

Asimismo, se establece la obligación de cada Administración de facilitar a las otras Administraciones los datos de los interesados que se le requieran y obren en su poder, en la tramitación de un procedimiento, siempre que el interesado preste su consentimiento expreso, el cual podrá emitirse y recabarse por medios electrónicos, al objeto de que los ciudadanos no deban aportar datos y documentos que están en poder de las Administraciones Públicas.

Para velar por la efectividad de los derechos reconocidos a los ciudadanos se prevé, en el ámbito de la Administración General del Estado, la actuación de las Inspecciones Generales de Servicios de los Departamentos Ministeriales y del Defensor del usuario.

En el Título Segundo se regula el régimen jurídico de la administración electrónica. Por una parte, su Capítulo Primero se dedica a la sede electrónica, como dirección electrónica cuya gestión y administración corresponde a una Administración Pública funcionando con plena responsabilidad respecto de la integridad, veracidad y actualización de la información y los servicios a los que puede accederse a través de la misma. En la normativa de desarrollo de la Ley, cada Administración determinará los instrumentos de creación de las sedes electrónicas.

En su Capítulo Segundo se regulan las formas de identificación y autenticación, tanto de los ciudadanos como de los órganos administrativos en el ejercicio de sus competencias, siendo destacable que se habilitan distintos instrumentos de acreditación, que se concretarán en la normativa aplicable a cada supuesto con criterios de proporcionalidad. El Documento Nacional de Identidad electrónico está habilitado con carácter general para todas las relaciones con las Administraciones Públicas, y por ello se impulsará como fórmula para extender el uso general de la firma electrónica. También se establece la obligación para cualquier Administración de admitir los certificados electrónicos reconocidos en el ámbito de la Ley de Firma Electrónica.

Interesa también destacar sobre esta cuestión, y con objeto de evitar la brecha digital, la posibilidad de que sean funcionarios públicos quienes acrediten la voluntad de los ciudadanos, siguiendo el procedimiento establecido, para sus relaciones electrónicas con la Administración.

En el Capítulo Tercero se regulan los registros, comunicaciones y notificaciones electrónicas. La principal novedad a este respecto es la nueva regulación de los registros electrónicos, de manera que puedan convertirse en un instrumento que se libere de la rigidez

actual y sirvan para la presentación de cualquier escrito o solicitud ante las Administraciones Públicas.

La Ley regula las comunicaciones electrónicas de los ciudadanos con las Administraciones y de éstas entre sí, para aunar los criterios de agilidad y de seguridad jurídica. En el Capítulo Cuarto, sobre los documentos y archivos electrónicos, se establecen las condiciones para reconocer la validez de un documento electrónico, se regula todo el sistema de copias electrónicas, tanto las realizadas a partir de documentos emitidos originariamente en papel, como las copias de documentos que ya estuvieran en soporte electrónico y las condiciones para realizar en soporte papel copia de originales emitidos por medios electrónicos, o viceversa.

El Título Tercero trata de la gestión electrónica de los procedimientos, desarrolla la regulación de los procedimientos administrativos utilizando medios electrónicos y los criterios a seguir en la gestión electrónica, guardando un cierto paralelismo con la regulación que encontramos en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Así, se regula la iniciación, instrucción y terminación de procedimientos por medios electrónicos.

En este Título cabe hacer especial referencia a la obligación que se establece para las Administraciones Públicas de poner a disposición de los usuarios información por medios electrónicos sobre el estado de tramitación de los procedimientos, tanto para los gestionados en su totalidad por medios electrónicos como para el resto de procedimientos.

El Título Cuarto está dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En él se establecen el órgano de cooperación en esta materia de la Administración General del Estado con los de las Comunidades Autónomas y con la Administración Local, y se determinan los principios para garantizar la interoperabilidad de sistemas de información así como las bases para impulsar la reutilización de aplicaciones y transferencia de tecnologías entre Administraciones.

La Ley consta, por último, de seis disposiciones adicionales, una transitoria, una derogatoria y ocho finales entre las que presenta especial relevancia la disposición final primera en la que se citan los preceptos de la ley que tienen carácter básico al amparo del artículo 149.1.18 de la Constitución.

Especial interés tiene también la disposición final tercera, pues con independencia de la fecha de entrada en vigor de la Ley, en ella se señalan las fechas para la efectividad plena del derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, estableciendo los plazos que se consideran adecuados para llevar a cabo las necesarias actuaciones previas de adecuación por parte de las distintas Administraciones Públicas.

TÍTULO PRELIMINAR

Del ámbito de aplicación y los principios generales

Artículo 1. *Objeto de la Ley.*

1. La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Artículo 2. *Ámbito de aplicación.*

1. La presente Ley, en los términos expresados en su disposición final primera, será de aplicación:

a) A las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

b) A los ciudadanos en sus relaciones con las Administraciones Públicas.

c) A las relaciones entre las distintas Administraciones Públicas.

2. La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado.

Artículo 3. *Finalidades de la Ley.*

Son fines de la presente Ley:

1. Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.

2. Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.

3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

4. Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.

5. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.

6. Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.

7. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.

Artículo 4. *Principios generales.*

La utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose a los siguientes principios:

a) El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.

b) Principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las Administraciones Públicas por medios no electrónicos, tanto respecto al acceso a la prestación de servicios públicos como respecto a cualquier actuación o procedimiento administrativo sin perjuicio de las medidas dirigidas a incentivar la utilización de los medios electrónicos.

c) Principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos de los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones, incorporando las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran.

d) Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley

30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

e) Principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar tanto la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas como, en su caso, la prestación conjunta de servicios a los ciudadanos. En particular, se garantizará el reconocimiento mutuo de los documentos electrónicos y de los medios de identificación y autenticación que se ajusten a lo dispuesto en la presente Ley.

f) Principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

g) 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. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

h) Principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos.

i) Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

j) Principio de simplificación administrativa, por el cual se reduzcan de manera sustancial los tiempos y plazos de los procedimientos administrativos, logrando una mayor eficacia y eficiencia en la actividad administrativa.

k) Principio de transparencia y publicidad del procedimiento, por el cual el uso de medios electrónicos debe facilitar la máxima difusión, publicidad y transparencia de las actuaciones administrativas.

Artículo 5. *Definiciones.*

A efectos de la presente ley, los términos que en ellas se emplean tendrán el sentido que se establece en su anexo.

TÍTULO PRIMERO

Derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos

Artículo 6. *Derechos de los ciudadanos.*

1. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, 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 las Administraciones Públicas.

b) A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.

c) A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.

d) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.

e) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.

f) A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.

g) A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.

h) A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.

i) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

j) A la calidad de los servicios públicos prestados por medios electrónicos.

k) A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

3. En particular, en los procedimientos relativos al acceso a una actividad de servicios y su ejercicio, los ciudadanos tienen derecho a la realización de la tramitación a través de una ventanilla única, por vía electrónica y a distancia, y a la obtención de la siguiente información a través de medios electrónicos, que deberá ser clara e inequívoca:

a) Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.

b) Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como los datos de las asociaciones y organizaciones distintas de las autoridades competentes a las que los prestadores o destinatarios puedan dirigirse para obtener asistencia o ayuda.

c) Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios.

d) Las vías de reclamación y recurso en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores.

Artículo 7. *Defensa de los derechos de los ciudadanos.*

1. En la Administración General del Estado, se crea la figura del Defensor del usuario de la administración electrónica, que velará por la garantía de los derechos reconocidos a los ciudadanos en la presente Ley, sin perjuicio de las competencias atribuidas en este ámbito a otros órganos o entidades de derecho público. Será nombrado por el Consejo de Ministros a propuesta del Ministro de Administraciones Públicas entre personas de reconocido prestigio en la materia. Estará integrado en el Ministerio de Administraciones Públicas y desarrollará sus funciones con imparcialidad e independencia funcional.

2. El Defensor del usuario de la administración electrónica elaborará, con carácter anual, un informe que se elevará al Consejo de Ministros y se remitirá al Congreso de los Diputados. Dicho informe contendrá un análisis de las quejas y sugerencia recibidas así como la propuesta de las actuaciones y medidas a adoptar en relación con lo previsto en el apartado 1 de este artículo.

3. Para el ejercicio de sus funciones, el Defensor del usuario de la administración electrónica contará con los recursos de la Administración General del Estado con la asistencia que, a tal efecto, le presten las Inspecciones Generales de los Servicios de los Departamentos ministeriales y la Inspección General de Servicios de la Administración Pública. En particular, las Inspecciones de los Servicios le asistirán en la elaboración del informe al que se refiere el apartado anterior y le mantendrán permanentemente informado de las quejas y sugerencias que se reciban en relación con la prestación de servicios públicos a través de medios electrónicos. A estos efectos, la Comisión Coordinadora de las Inspecciones generales de servicios de los departamentos ministeriales realizará, en este ámbito, las funciones de coordinación que tiene legalmente encomendadas.

4. Reglamentariamente se determinará el estatuto del Defensor del usuario de la administración electrónica, así como la regulación de sus relaciones con los órganos a los que se refiere el apartado anterior de este artículo.

Artículo 8. *Garantía de prestación de servicios y disposición de medios e instrumentos electrónicos.*

1. Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando 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. La Administración General del Estado garantizará 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 atención presencial que se determinen, las cuales pondrán a disposición de los ciudadanos de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 6 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 electrónicas creadas y gestionadas por los departamentos y organismos públicos y disponibles para los ciudadanos a través de redes de comunicación. En particular se creará un Punto de acceso general a través del cual los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles. Este Punto de acceso general contendrá la relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.

c) Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores.

Artículo 9. *Transmisiones de datos entre Administraciones Públicas.*

1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley.

TÍTULO SEGUNDO

Régimen jurídico de la administración electrónica

CAPÍTULO I

De la sede electrónica

Artículo 10. *La sede electrónica.*

1. La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

Artículo 11. *Publicaciones electrónicas de Boletines Oficiales.*

1. La publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tendrá, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.

2. La publicación del «Boletín Oficial del Estado» en la sede electrónica del organismo competente 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.

Artículo 12. *Publicación electrónica del tablón de anuncios o edictos.*

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.

CAPÍTULO II

De la identificación y autenticación

Sección 1.ª Disposiciones comunes

Artículo 13. *Formas de identificación y autenticación.*

1. Las Administraciones Públicas admitirán, 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 participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

a) En todo caso, 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. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.

b) Sistemas de firma electrónica para la actuación administrativa automatizada.

c) Firma electrónica del personal al servicio de las Administraciones Públicas.

d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

Sección 2.ª Identificación de los ciudadanos y autenticación de su actuación

Artículo 14. *Utilización del Documento Nacional de Identidad.*

Las personas físicas podrán, en todo caso y con carácter universal, utilizar los sistemas de firma electrónica incorporados al Documento Nacional de Identidad en su relación por medios electrónicos con las Administraciones Públicas. El régimen de utilización y efectos de dicho documento se regirá por su normativa reguladora.

Artículo 15. *Utilización de sistemas de firma electrónica avanzada.*

1. Los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, referidos en el artículo 14, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos.

2. La relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada Administración Pública, deberá ser pública y accesible por medios electrónicos. Dicha relación incluirá, al menos, información sobre los elementos de identificación utilizados así como, en su caso, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados.

3. Los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que estas determinen.

Artículo 16. *Utilización de otros sistemas de firma electrónica.*

1. Las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.

2. En aquellos supuestos en los que se utilicen estos sistemas para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública, ésta deberá garantizar la integridad y el no repudio por ambas partes de los documentos electrónicos concernidos.

3. Cuando resulte preciso, las Administraciones Públicas certificarán la existencia y contenido de las actuaciones de los ciudadanos en las que se hayan usado formas de identificación y autenticación a que se refiere este artículo.

Sección 3.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia

Artículo 17. *Identificación de las sedes electrónicas.*

Las sedes 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.

Artículo 18. *Sistemas de firma electrónica para la actuación administrativa automatizada.*

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Los certificados electrónicos a los que se hace referencia en el apartado 1.a) incluirán el número de identificación fiscal y la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

3. 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. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

Artículo 19. *Firma electrónica del personal al servicio de las Administraciones Públicas.*

1. Sin perjuicio de lo previsto en los artículos 17 y 18, la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad 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. Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales 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. La firma electrónica basada en el Documento Nacional de Identidad podrá utilizarse a los efectos de este artículo.

Artículo 20. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, 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 una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas administraciones, 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.

Sección 4.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos

Artículo 21. *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 las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

2. Los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad.

3. La Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones. Cada Administración Pública podrá disponer de los mecanismos necesarios para la verificación del estado de revocación y la firma con los certificados electrónicos admitidos en su ámbito de competencia.

Artículo 22. *Identificación y autenticación de los ciudadanos por funcionario público.*

1. En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 13 de los que aquel no disponga, tal identificación o autenticación podrá ser validamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

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.

3. Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación regulada en este artículo.

Artículo 23. *Formas de Representación.*

Sin perjuicio de lo dispuesto en el artículo 13.2, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. Dicha habilitación deberá especificar las condiciones y obligaciones a las que se comprometen los que así adquieran la condición de representantes, y determinará la presunción de validez de la representación salvo que la normativa de aplicación prevea otra cosa. Las Administraciones Públicas podrán requerir, en cualquier momento, la acreditación de dicha representación.

CAPÍTULO III

De los registros, las comunicaciones y las notificaciones electrónicas

Sección 1.ª De los Registros

Artículo 24. *Registros electrónicos.*

1. Las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

2. Los registros electrónicos podrán admitir:

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 apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

3. En cada Administración Pública existirá, al menos, un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidos a dicha Administración Pública. Las Administraciones Públicas podrán, mediante convenios de colaboración, habilitar a sus respectivos registros para la recepción de las solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio.

4. En el ámbito de la Administración General del Estado se automatizarán las oficinas de registro físicas a las que se refiere el artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, a fin de garantizar la interconexión de todas sus oficinas y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

Artículo 25. *Creación y funcionamiento.*

1. Las disposiciones de creación de registros electrónicos se publicarán en el Diario Oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles a los efectos previstos en el artículo siguiente.

2. En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones a las que se refiere el apartado 2.a) del artículo anterior que pueden presentarse en el mismo así como, en su caso, la posibilidad de presentación de solicitudes, escritos y comunicaciones a los que se refiere el apartado 2.b) de dicho artículo.

3. Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

4. Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.

Artículo 26. *Cómputo de plazos.*

1. Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las Administraciones Públicas por la fecha y hora oficial de la sede 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 solicitudes, escritos 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 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 los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado 2.b del artículo 24, por la fecha y hora de entrada en el registro del destinatario. En todo caso, la fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el escrito, solicitud o comunicación.

5. Cada sede electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquella, los días que se considerarán inhábiles a los efectos de los apartados anteriores. En todo caso, no será de aplicación a los registros electrónicos lo dispuesto en el artículo 48.5 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Sección 2.ª De las comunicaciones y las notificaciones electrónicas

Artículo 27. *Comunicaciones electrónicas.*

1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.

2. Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos.

3. Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.

4. Las Administraciones publicarán, en el correspondiente Diario Oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con ellas.

5. 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.

6. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con 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.

7. Las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas. Las condiciones que regirán estas comunicaciones se determinarán entre las Administraciones Públicas participantes.

Artículo 28. *Práctica de la notificación por medios electrónicos.*

1. Para que la notificación se practique utilizando algún medio electrónico se requerirá que el interesado haya señalado dicho medio como preferente o haya consentido su utilización, sin perjuicio de lo dispuesto en el artículo 27.6. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citados anteriormente podrán emitirse y recabarse, en todo caso, por medios electrónicos.

2. El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.

3. Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el artículo 59.4 de la Ley 30/1992 de Régimen Jurídico y del Procedimiento Administrativo Común y normas concordantes, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.

4. Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, de Régimen Jurídico y del Procedimiento Administrativo Común, excepto en los casos previstos en el artículo 27.6 de la presente Ley.

5. Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dichos acceso.

CAPÍTULO IV

De los documentos y los archivos electrónicos

Artículo 29. *Documento administrativo electrónico.*

1. Las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Sección 3.ª del Capítulo II de la presente Ley.

2. Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

3. La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

Artículo 30. *Copias electrónicas.*

1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

2. Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Las Administraciones Públicas 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. En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá

procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

5. Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

Artículo 31. *Archivo electrónico de documentos.*

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

2. Los documentos electrónicos que contengan actos administrativos 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. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Artículo 32. *Expediente electrónico.*

1. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

2. El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

3. La remisión de expedientes podrá ser sustituida a todos los efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo.

TÍTULO TERCERO

De la gestión electrónica de los procedimientos

CAPÍTULO I

Disposiciones comunes

Artículo 33. *Utilización de medios electrónicos.*

1. La gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa.

2. En la aplicación de medios electrónicos a la actividad administrativa se considerará la adecuada dotación de recursos y medios materiales al personal que vaya a utilizarlos, así como la necesaria formación acerca de su utilización.

Artículo 34. *Criterios para la gestión electrónica.*

La aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio, en el que se considerarán especialmente los siguientes aspectos:

a) La supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regulación de su aportación al finalizar la tramitación.

b) La previsión de medios e instrumentos de participación, transparencia e información.

c) La reducción de los plazos y tiempos de respuesta.

d) La racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas.

CAPÍTULO II

Utilización de medios electrónicos en la tramitación del procedimiento

Artículo 35. *Iniciación del procedimiento por medios electrónicos.*

1. La iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares en los términos establecidos en el apartado i) del artículo 4 y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

2. Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos.

3. Con objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso, ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete.

Artículo 36. *Instrucción del procedimiento utilizando medios electrónicos.*

1. Las aplicaciones y sistemas de información utilizados para la instrucción por medios electrónicos de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación de los órganos responsables 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 los órganos y unidades intervinientes a efectos de emisión y recepción de informes u otras actuaciones deberán cumplir los requisitos establecidos en esta Ley.

3. Cuando se utilicen medios electrónicos para la participación de los interesados en la instrucción del procedimiento a los efectos del ejercicio de su derecho a presentar alegaciones en cualquier momento anterior a la propuesta de resolución o en la práctica del trámite de audiencia cuando proceda, se emplearán los medios de comunicación y notificación previstos en los artículos 27 y 28 de esta Ley.

Artículo 37. *Acceso de los interesados a la información sobre el estado de tramitación.*

1. En los procedimientos administrativos gestionados en su totalidad electrónicamente, el órgano que tramita el procedimiento pondrá a disposición del interesado un servicio electrónico de acceso restringido donde éste pueda consultar, previa identificación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información. 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.

2. En el resto de los procedimientos se habilitarán igualmente servicios electrónicos de información del estado de la tramitación que comprendan, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable.

Artículo 38. *Terminación de los procedimientos por medios electrónicos.*

1. La resolución de un procedimiento utilizando medios electrónicos garantizará la identidad del órgano competente mediante el empleo de alguno de los instrumentos previstos en los artículos 18 y 19 de esta Ley.

2. Podrán adoptarse y notificarse resoluciones de forma automatizada en aquellos procedimientos en los que así esté previsto.

Artículo 39. *Actuación administrativa automatizada.*

En caso de actuación automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

TÍTULO CUARTO

Cooperación entre administraciones para el impulso de la administración electrónica

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 40. *Comité Sectorial de administración electrónica.*

1. El Comité Sectorial de administración electrónica, dependiente de la Conferencia Sectorial de Administración Pública, es el órgano técnico de cooperación de la Administración General del Estado, de las administraciones de las Comunidades Autónomas y de las entidades que integran la Administración Local en materia de administración electrónica.

2. El Comité Sectorial de la administración electrónica velará por el cumplimiento de los fines y principios establecidos en esta Ley, y en particular desarrollará las. siguientes funciones:

a) Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas.

b) Preparar planes programas conjuntos de actuación para impulsar el desarrollo de la administración electrónica en España.

c) Asegurar la cooperación entre las administraciones públicas para proporcionar al ciudadano información administrativa clara, actualizada e inequívoca.

3. Cuando por razón de las materias tratadas resulte de interés podrá invitarse a las organizaciones, corporaciones o agentes sociales que se estime conveniente en cada caso a participar en las deliberaciones del comité sectorial.

CAPÍTULO II

Cooperación en materia de interoperabilidad de sistemas y aplicaciones

Artículo 41. *Interoperabilidad de los Sistemas de Información.*

Las Administraciones Públicas utilizarán las tecnologías de la información en sus relaciones con las demás administraciones y con los ciudadanos, aplicando medidas informáticas, tecnológicas, 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.

Artículo 42. *Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.*

1. El Esquema Nacional de Interoperabilidad comprenderá 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.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3. Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.

4. En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos considerarán la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

Artículo 43. *Red de comunicaciones de las Administraciones Públicas españolas.*

La Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

Artículo 44. *Red integrada de Atención al Ciudadano.*

1. Las Administraciones Públicas podrán suscribir convenios de colaboración con objeto de articular medidas e instrumentos de colaboración para la implantación coordinada y normalizada de una red de espacios comunes o ventanillas únicas.

2. En particular, y de conformidad con lo dispuesto en el apartado anterior, se implantarán espacios comunes o ventanillas únicas para obtener la información prevista en el artículo 6.3 de esta Ley y para realizar los trámites y procedimientos a los que hace referencia el apartado a) de dicho artículo.

CAPÍTULO III

Reutilización de aplicaciones y transferencia de tecnologías

Artículo 45. *Reutilización de sistemas y aplicaciones de propiedad de la Administración.*

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 Administración 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 Pública o se fomente la incorporación de los ciudadanos a la Sociedad de la información

Artículo 46. *Transferencia de tecnología entre Administraciones.*

1. Las Administraciones Públicas 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 Esquema Nacional de Interoperabilidad.

2. La Administración General del Estado, a través de un centro para la transferencia de la tecnología, mantendrá un directorio general de aplicaciones para su reutilización, prestará asistencia técnica para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes de especial interés para el desarrollo de la administración electrónica en el marco de los esquemas nacionales de interoperabilidad y seguridad.

Disposición adicional primera. *Reunión de Órganos colegiados por medios electrónicos.*

1. Los órganos colegiados podrán constituirse y adoptar acuerdos utilizando medios electrónicos, con respeto a los trámites esenciales establecidos en los artículos 26 y el 27.1 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. En la Administración General del Estado, lo previsto en el apartado anterior se efectuará de acuerdo con las siguientes especialidades:

a) Deberá garantizarse la realización efectiva de los principios que la legislación establece respecto de la convocatoria, acceso a la información y comunicación del orden del día, en donde se especificarán los tiempos en los que se organizarán los debates, la formulación y conocimiento de las propuestas y la adopción de acuerdos.

b) El régimen de constitución y adopción de acuerdos garantizará la participación de los miembros de acuerdo con las disposiciones propias del órgano.

c) Las actas garantizarán la constancia de las comunicaciones producidas así como el acceso de los miembros al contenido de los acuerdos adoptados.

Disposición adicional segunda. *Formación de empleados públicos.*

La Administración General del Estado promoverá la formación del personal a su servicio en la utilización de medios electrónicos para el desarrollo de las actividades propias de aquélla.

En especial, los empleados públicos de la Administración General del Estado recibirán formación específica que garantice conocimientos actualizados de las condiciones de seguridad de la utilización de medios electrónicos en la actividad administrativa, así como de protección de los datos de carácter personal, respeto a la propiedad intelectual e industrial y gestión de la información.

Disposición adicional tercera. *Plan de Medios en la Administración General del Estado.*

En el plazo de seis meses a partir de la publicación de esta Ley, el Ministerio de Administraciones Públicas, en colaboración con los Ministerios de Economía y Hacienda y de Industria, Turismo y Comercio, elevará al Consejo de Ministros un Plan de implantación de los medios necesarios para el ámbito de la Administración General del Estado. Dicho Plan incorporará las estimaciones de los recursos económicos, técnicos y humanos que se consideren precisos para la adecuada aplicación de lo dispuesto en la presente Ley en los tiempos establecidos en el calendario al que se refiere el apartado 2 de la disposición final tercera, así como los mecanismos de evaluación y control de su aplicación.

Disposición adicional cuarta. *Procedimientos Especiales.*

La aplicación de lo dispuesto en el Título Tercero de esta ley a los procedimientos en materia tributaria, de seguridad social y desempleo y de régimen jurídico de los extranjeros en España, se efectuará de conformidad con lo establecido en las disposiciones adicionales quinta, sexta, séptima y decimonovena de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Asimismo, en la aplicación de esta ley habrán de ser tenidas en cuenta las especificidades en materia de contratación pública, conforme a lo preceptuado en la disposición adicional séptima del Texto Refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto Legislativo 2/2000, de 16 de junio.

Disposición adicional quinta. *Función Estadística.*

Lo dispuesto en los artículos 6.2.b) y 9 de la presente ley no será de aplicación a la recogida de datos prevista en el Capítulo II de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

Disposición adicional sexta. *Uso de Lenguas Oficiales.*

1. Se garantizará el uso de las lenguas oficiales del Estado en las relaciones por medios electrónicos de los ciudadanos con las Administraciones Públicas, en los términos previstos en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en la normativa que en cada caso resulte de aplicación.

2. A estos efectos, las sedes electrónicas cuyo titular tenga competencia sobre territorios con régimen de cooficialidad lingüística posibilitarán el acceso a sus contenidos y servicios en las lenguas correspondientes.

3. Los sistemas y aplicaciones utilizados en la gestión electrónica de los procedimientos se adaptarán a lo dispuesto en cuanto al uso de lenguas cooficiales en el artículo 36 de la ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común.

4. Cada Administración Pública afectada determinará el calendario para el cumplimiento progresivo de lo previsto en la presente disposición, debiendo garantizar su cumplimiento total en los plazos establecidos en la disposición final tercera.

Disposición transitoria única. *Régimen Transitorio.*

1. Los procedimientos y actuaciones de los ciudadanos y las Administraciones Públicas que, utilizando medios electrónicos, se hayan iniciado con anterioridad a la entrada en vigor de la presente Ley se seguirán rigiendo por la normativa anterior hasta su terminación.

2. Los registros telemáticos existentes a la entrada en vigor de la presente Ley serán considerados registros electrónicos regulándose por lo dispuesto en los artículos 24, 25 y 26 de esta Ley.

Disposición derogatoria única.

1. Quedan derogados los siguientes preceptos de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común: apartado

número 9 del artículo 38, apartados números 2, 3 y 4 del artículo 45, apartado número 3 del artículo 59 y la disposición adicional decimoctava.

2. Asimismo, quedan derogadas las normas de igual o inferior rango en cuanto contradigan o se opongan a lo dispuesto en la presente Ley.

Disposición final primera. *Carácter básico de la Ley.*

1. Los artículos 1, 2, 3, 4, 5, 6, 8.1, 9, 10, 11.1, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21.1,21.2, 22, 23, 24.1, 24.2, 24.3, 25, 26, 27, 28, 29.1, 29.2, 30, 32, 35, 37.1, 38, 42, el apartado 1 de la disposición adicional primera, la disposición adicional cuarta, la disposición transitoria única y la disposición final tercera se dictan al amparo de lo dispuesto 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 y sobre el procedimiento administrativo común.

2. Con excepción del artículo 42, el Título IV de la presente ley será de aplicación a todas las Administraciones Públicas en la medida en que éstas participen o se adscriban a los órganos de cooperación o instrumentos previstos en el mismo.

Disposición final segunda. *Publicación electrónica del «Boletín Oficial del Estado».*

La publicación electrónica del «Boletín Oficial del Estado» tendrá el carácter y los efectos previstos en el artículo 11.2 de la presente Ley desde el 1 de enero de 2009.

Disposición final tercera. *Adaptación de las Administraciones Públicas para el ejercicio de derechos.*

1. Desde la fecha de entrada en vigor de la presente Ley, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con los procedimientos y actuaciones adaptados a lo dispuesto en la misma, sin perjuicio de lo señalado en los siguientes apartados. A estos efectos, cada Administración Pública hará pública y mantendrá actualizada la relación de dichos procedimientos y actuaciones.

2. En el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009. A tal fin, el Consejo de Ministros establecerá y hará público un calendario de adaptación gradual de aquellos procedimientos y actuaciones que lo requieran.

3. En el ámbito de las Comunidades Autónomas, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias.

4. En el ámbito de las Entidades que integran la Administración Local, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias. A estos efectos las Diputaciones Provinciales, o en su caso los Cabildos y Consejos Insulares u otros organismos supramunicipales, podrán prestar los servicios precisos para garantizar tal efectividad en el ámbito de los municipios que no dispongan de los medios técnicos y organizativos necesarios para prestarlos.

5. Las Comunidades Autónomas y las Entidades integradas en la Administración Local en las que no puedan ser ejercidos a partir del 31 de diciembre de 2009 los derechos reconocidos en el artículo 6 de la presente Ley, en relación con la totalidad de los procedimientos y actuaciones de su competencia, deberán aprobar y hacer públicos los programas y calendarios de trabajo precisos para ello, atendiendo a las respectivas previsiones presupuestarias, con mención particularizada de las fases en las que los diversos derechos serán exigibles por los ciudadanos.

Los anteriores programas podrán referirse a una pluralidad de municipios cuando se deban ejecutar en aplicación de los supuestos de colaboración previstos en el apartado anterior.

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.*

Uno. El apartado 2 del artículo 4 queda redactado del siguiente modo:

«2. Quienes hubieran de renovar preceptivamente su documento durante el plazo de vigencia del mismo, por variación de alguno de los datos que se recogen en el mismo.»

Dos. El artículo 6 queda redactado del siguiente modo:

«Artículo 6. *Cuota tributaria.*

La cuota tributaria exigible será de 6,70 euros. Los excesos del costo de la expedición, si existen, serán sufragados con cargo a los Presupuestos Generales del Estado.»

Disposición final quinta. *Modificación de la Ley 16/1979, de 2 de octubre, sobre Tasas de la Jefatura Central de Tráfico.*

Uno. En el apartado 1 del artículo 5 se modifica la letra d) y se incorpora una nueva letra e) que quedan redactadas del siguiente modo:

«d) Quienes soliciten duplicados de las autorizaciones administrativas para conducir o para circular por cambio de domicilio.

e) Quienes soliciten la baja definitiva de un vehículo por entrega en un establecimiento autorizado para su destrucción.»

Dos. Los puntos 4 y 4 bis, primera columna de la izquierda del Grupo IV del artículo 6, quedan redactados del siguiente modo:

«4. Duplicados de permisos, autorizaciones por extravío, sustracción, deterioro, prórroga de vigencia o cualquier modificación de aquéllos.

4 bis. duplicados de licencias de conducción y de circulación de ciclomotores por extravío, sustracción, deterioro, prórroga de vigencia o cualquier modificación de aquéllos.»

Disposición final sexta. *Habilitación para la regulación del teletrabajo en la Administración General del Estado.*

El Ministerio de Administraciones Públicas, en colaboración con los Ministerios de Economía y Hacienda, de Industria, Turismo y Comercio y de Trabajo y Asuntos Sociales, regularán antes del 1 de marzo de 2008 las condiciones del teletrabajo en la Administración General del Estado.

Disposición final séptima. *Desarrollo reglamentario del artículo 4.c).*

El Gobierno desarrollará reglamentariamente lo previsto en el artículo 4.c) de la presente Ley para garantizar que todos los ciudadanos, con especial atención a las personas con algún tipo de discapacidad y mayores, que se relacionan con la Administración General del Estado puedan acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos.

Disposición final octava. *Desarrollo y entrada en vigor de la Ley.*

1. 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.

2. 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:

a) Actuación administrativa automatizada: Actuación administrativa 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.

b) Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

c) 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.

d) 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.

e) 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).

f) 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».

g) 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 presten».

h) Ciudadano: Cualesquiera personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones Públicas.

i) Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

j) 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.

k) 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.

l) Firma electrónica: Según el 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».

m) Firma electrónica avanzada: Según el 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».

n) Firma electrónica reconocida: Según el 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».

o) 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.

p) 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.

q) 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 a una institución pública.

r) 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.

s) 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.

t) 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.

u) Actividad de servicio: Cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración.

v) Prestador de actividad de servicio: Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

§ 2

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

Ministerio de la Presidencia
«BOE» núm. 278, de 18 de noviembre de 2009
Última modificación: sin modificaciones
Referencia: BOE-A-2009-18358

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, marca un hito trascendental en la construcción de la Administración pública de la sociedad de la información en España. Aunque apoyada en la experiencia adquirida con la aplicación de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común, en cuyos artículos 38, 45, 46 y 59, principalmente, ofrecía un marco jurídico general de referencia para la incorporación sistemática de las tecnologías de la información y de las comunicaciones a las funciones administrativas, así como en el avance que supuso la promulgación de la Ley 58/2003, de 17 de diciembre, General Tributaria, al recoger por primera vez la automatización de la actuación administrativa o la obtención de imágenes electrónicas de los documentos con idéntica validez y eficacia que el documento origen, lo cierto es que la Ley 11/2007, de 22 de junio, desborda el papel de solución de desarrollo o consolidación de la anterior por significar un verdadero replanteamiento de la relación entre la Administración y los ciudadanos.

La Ley 11/2007, de 22 de junio, impulsa una nueva concepción al construir su regulación sobre la base del derecho de los ciudadanos a utilizar los medios de comunicación electrónica para relacionarse con la Administración y ejercer sus derechos. Este singular punto de partida que pone al ciudadano y sus derechos en la base de todo, no sólo significa la imposición de un compromiso jurídico de incorporar las tecnologías de la información a la totalidad de las funciones administrativas. También, implica la consideración del ciudadano como portador de derechos de prestación que la Administración debe satisfacer de forma efectiva. Por ello, la ley estableció un elenco de derechos específicamente relacionados con la comunicación electrónica con la Administración y con su estatuto de ciudadano: derecho a la obtención de medios de identificación electrónica, derecho a elección del canal de comunicación o del medio de autentificación y de igualdad garantizando la accesibilidad, así como una efectiva igualdad entre géneros y respecto de otros colectivos con necesidades especiales y entre territorios.

Esta ambiciosa estrategia se ha asumido con una gran decisión. La disposición final tercera de la Ley 11/2007, de 22 de junio, establece la fecha del 31 de diciembre de 2009, como límite para que los ciudadanos puedan ejercer con plenitud sus derechos por medios electrónicos en cualquier procedimiento y actividad de competencia de dicha Administración.

El cumplimiento de los objetivos legales establecidos por la Ley 11/2007, de 22 de junio, y de los plazos previstos para su efectividad, justifican la necesidad de desarrollo de sus previsiones, en la medida que:

a) La Ley 11/2007, de 22 de junio, no agotó la regulación del acceso electrónico a los servicios públicos como consecuencia de los criterios de distribución de competencias y su incidencia en las competencias de autoorganización que corresponde al resto de las Administraciones públicas.

b) Por otro lado, por su carácter trasversal, esta regulación presupone operaciones de adaptación a los distintos procedimientos y actividades. El cumplimiento de esta necesidad solo puede lograrse mediante la previsión de un sistema de regulación caracterizado por la concurrencia de diferentes niveles normativos y la colaboración entre ellos para componer un marco general, objetivo, estable y predecible compatible con la adaptación funcional y con el estado del desarrollo tecnológico en esta materia.

El presente real decreto pretende ser ese complemento necesario en la Administración General del Estado para facilitar la efectiva realización de los derechos reconocidos en la Ley 11/2007, de 22 de junio.

Este real decreto se ha construido sobre la base de los siguientes principios estratégicos:

a) En primer lugar, procurar la más plena realización de los derechos reconocidos en la Ley 11/2007, de 22 de junio, facilitándolos en la medida que lo permite el estado de la técnica, y la garantía de que no resultan afectados otros bienes constitucionalmente protegidos, como pueden ser la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros.

b) En segundo lugar, establecer un marco lo más flexible posible en la implantación de los medios de comunicación, cuidando los niveles de seguridad y protección de derechos e intereses previstos tanto en la propia Ley 11/2007, de 22 de junio, como en la legislación administrativa en general. Con ello se persigue un triple objetivo: en primer lugar, evitar que la nueva regulación imponga una renovación tal en las soluciones de comunicación con los ciudadanos que impida la pervivencia de técnicas existentes y de gran arraigo; en segundo lugar, facilitar la actividad de implantación y adaptación a las distintas organizaciones, funciones y procedimientos a los que es de aplicación el real decreto; y en tercer lugar, impedir que la opción rígida por determinadas soluciones dificulte para el futuro la incorporación de nuevas soluciones y servicios.

No obstante, la realización de estos objetivos requiere de otros dos instrumentos de carácter técnico y complementario: el Esquema Nacional de Interoperabilidad, encargado de establecer los criterios comunes de gestión de la información que permitan compartir soluciones e información, y el Esquema Nacional de Seguridad que deberá establecer los criterios y niveles de seguridad necesarios para los procesos de tratamiento de la información que prevé el propio real decreto.

Fiel a esta orientación, el real decreto incorpora en su frontispicio una regulación específica destinada a hacer efectivo el derecho a no incorporar documentos que se encuentren en poder de las Administraciones públicas, estableciendo las reglas necesarias para obtener los datos y documentos exigidos, con las garantías suficientes que impidan que esta facilidad se convierta, en la práctica, en un motivo de retraso en la resolución de los procedimientos administrativos.

A estos efectos, se regula la forma y los efectos del ejercicio del derecho por parte de los ciudadanos, se contemplan los distintos supuestos que se pueden dar en cuanto a la obtención de los datos o documentos, se establecen plazos obligatorios para atender dichos requerimientos, así como el deber de informar sobre la demora en su cumplimiento para que el interesado pueda suplir la falta de actividad del órgano o entidad requerida, sin perjuicio de exigir las responsabilidades que, en su caso, procedan.

Un elemento clave en la comunicación jurídica con los ciudadanos en soporte electrónico es el concepto de sede electrónica. En este punto el real decreto pretende reforzar la fiabilidad de estos puntos de encuentro mediante tres tipos de medidas: 1) asegurar la plena identificación y diferenciación de estas direcciones como punto de prestación de servicios de comunicación con los interesados, 2) establecer el conjunto de servicios característicos así

como el alcance de su eficacia y responsabilidad, y 3) imponer un régimen común de creación de forma que se evite la desorientación que para el ciudadano podría significar una excesiva dispersión de tales direcciones. Este régimen de la sede, que debe resultar compatible con la descentralización necesaria derivada de la actual complejidad de fines y actividades asumidas por la Administración, resulta, sin embargo, compatible con la creación de un punto de acceso común a toda la Administración, puerta de entrada general del ciudadano a la Administración, en la que éste podrá presentar sus comunicaciones electrónicas generales o encontrar la información necesaria para acudir a las sedes electrónicas en las que iniciar o participar en los procedimientos que por ser tramitados en soporte electrónico, requieren el acceso a aplicaciones o formularios concretos.

En materia de identificación y autenticación el real decreto ha pretendido establecer los elementos mínimos imprescindibles para afianzar el criterio de flexibilización impulsado en la Ley 11/2007, de 22 de junio, en la que junto a la admisión como medio universal de los dispositivos de identificación y firma electrónica asociados al documento nacional de identidad, se admite la utilización de otros medios de autenticación que cumplan con las condiciones de seguridad y certeza necesarias para el normal desarrollo de la función administrativa.

Asimismo se ha previsto un régimen específico que facilita la actuación en nombre de terceros a través de dos mecanismos fundamentales: por un lado, la figura de las habilitaciones generales y especiales, pensadas fundamentalmente para el desempeño continuado y profesional de actividades de gestión y representación ante los servicios de la Administración, así como un registro voluntario de representantes, también pensado con la finalidad de facilitar el ejercicio de la función de representación, estableciendo un mecanismo de acreditación en línea del título previamente aportado a dicho registro.

El real decreto especifica igualmente las previsiones contenidas en la ley, en cuanto a la posibilidad de que los funcionarios públicos habilitados al efecto puedan realizar determinas operaciones por medios electrónicos usando sus propios sistemas de identificación y autenticación en aquellos casos en que los ciudadanos no dispongan de medios propios.

La relevancia jurídica de la actividad administrativa ha exigido prestar una atención singularizada al uso de los medios de identificación y autenticación electrónica por parte de la Administración, estableciendo la necesidad de incorporación de sellos o marcas de tiempo, que acrediten la fecha de adopción de los actos y documentos que se emitan. Igualmente se ha dispensado una atención especial a la autenticación en el seno de la actuación automatizada.

Por último se incorporan unas previsiones destinadas a garantizar la interoperabilidad y efectividad del sistema de la ley entre las que se incluye un reconocimiento expreso a las políticas de firma que serán los instrumentos encargados de especificar las soluciones técnicas y de organización necesarias para la plena operatividad de los derechos reconocidos en la ley, un sistema nacional de verificación de certificados dispuesto para simplificar y agilizar las operaciones de comprobación de la vigencia de los certificados.

En materia de registros electrónicos se han desarrollado las previsiones de la ley con la importante novedad de la creación de un registro electrónico común que posibilitará a los ciudadanos la presentación de comunicaciones electrónicas para cualquier procedimiento y órganos de los integrados en la Administración General del Estado y sus organismos públicos dependientes o vinculados.

Esta misma línea de desarrollo indispensable de las previsiones de la ley se ha seguido en relación con las comunicaciones y notificaciones electrónicas, estableciendo las garantías necesarias para que las facilidades incluidas en la Ley 11/2007, de 22 de junio, no se conviertan en una desventaja para los intereses de los ciudadanos así como del interés general.

Por último, uno de los puntos esenciales de la disciplina de la ley es la regulación de la gestión de la información electrónica aportada por los particulares, previéndose las condiciones mínimas para que su utilización no afecte al desarrollo de las funciones administrativas. Resulta especialmente innovadora la previsión en nuestro ordenamiento de un régimen de gestión y cambio de soporte con el fin de facilitar la gestión de los expedientes por la opción del órgano encargado de su tramitación del soporte tipo en el que deberá tramitarse el procedimiento. Igualmente el real decreto es consciente de la

importancia de integrar, desde la misma incorporación de los documentos, de aquella información que permita su gestión, archivo y recuperación. Asimismo, el real decreto, al regular los procesos de destrucción de documentos en papel que son objeto de copiado electrónico, establece un sistema reforzado de garantías con particular atención a la conservación de los documentos con valor histórico.

El presente real decreto se dicta en virtud de la habilitación expresa al Gobierno contenida en la disposición final séptima de la Ley 11/2007, de 22 de junio, y ha sido informado por la Agencia Española de Protección de Datos, el Consejo Superior de Administración Electrónica y el Consejo de Consumidores y Usuarios.

En su virtud, a propuesta de las Ministras de la Presidencia y de Economía y Hacienda y 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 6 de noviembre de 2009,

DISPONGO:

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente real decreto tiene por objeto desarrollar la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos en el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, en lo relativo a la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones y documentos electrónicos y copias.

2. Sus disposiciones son de aplicación:

a) A la actividad de la Administración General del Estado, así como de los organismos públicos vinculados o dependientes de la misma.

b) A los ciudadanos en sus relaciones con las entidades referidas en el párrafo anterior.

c) A las relaciones entre los órganos y organismos a los que se refiere el párrafo a).

Artículo 2. *Transmisiones de datos y documentos, incluidos certificados, entre órganos y organismos de la Administración General del Estado con ocasión del ejercicio reconocido por el artículo 6.2.b) de la Ley 11/2007, de 22 de junio.*

1. Cuando los ciudadanos ejerzan el derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas establecido en el artículo 6.2.b) de la Ley 11/2007, de 22 de junio, ante los órganos administrativos incluidos en el ámbito de aplicación del apartado 2.a) del artículo 1, de este real decreto, se seguirán las siguientes reglas:

a) La Administración facilitará a los interesados en los procedimientos administrativos el ejercicio del derecho, que podrá efectuarse por medios electrónicos.

En todo caso, los interesados serán informados expresamente de que el ejercicio del derecho implica su consentimiento, en los términos establecidos por el artículo 6. 2b) de la Ley 11/2007, de 22 de junio, para que el órgano y organismo ante el que se ejercita pueda recabar los datos o documentos respecto de los que se ejercita el derecho de los órganos u organismos en que los mismos se encuentren.

El derecho se ejercitará de forma específica e individualizada para cada procedimiento concreto, sin que el ejercicio del derecho ante un órgano u organismo implique un consentimiento general referido a todos los procedimientos que aquel tramite en relación con el interesado.

b) En cualquier momento, los interesados podrán aportar los datos o documentos o certificados necesarios, así como revocar su consentimiento para el acceso a datos de carácter personal.

c) Si el órgano administrativo encargado de la tramitación del procedimiento, posee, en cualquier tipo de soporte, los datos, documentos o certificados necesarios o tiene acceso electrónico a los mismos, los incorporará al procedimiento administrativo correspondiente sin más trámite. En todo caso, quedará constancia en los ficheros del órgano u organismo cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario.

d) Cuando el órgano administrativo encargado de la tramitación del procedimiento no tenga acceso a los datos, documentos o certificados necesarios, los pedirá al órgano administrativo correspondiente. Si se tratara de un órgano administrativo incluido en el ámbito de aplicación del artículo 1.2.a), deberá ceder por medios electrónicos los datos, documentos y certificados que sean necesarios en el plazo máximo que establezca la normativa específica, que no podrá exceder de diez días. Dicho plazo máximo será igualmente aplicable si no está fijado en la normativa específica.

e) En caso de imposibilidad de obtener los datos, documentos o certificados necesarios por el órgano administrativo encargado de la tramitación del procedimiento, se comunicará al interesado con indicación del motivo o causa, para que los aporte en el plazo y con los efectos previstos en la normativa reguladora del procedimiento correspondiente. En este caso, el interesado podrá formular queja conforme con lo previsto en el Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

f) Los órganos u organismos ante los que se ejercite el derecho conservarán la documentación acreditativa del efectivo ejercicio del derecho incorporándola al expediente en que el mismo se ejerció.

Dicha documentación estará a disposición del órgano cedente y de las autoridades a las que en su caso corresponda la supervisión y control de la legalidad de las cesiones producidas.

2. El Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad establecerán las previsiones necesarias para facilitar el ejercicio de este derecho por los ciudadanos.

3. A fin de dar cumplimiento a la exigencia del artículo 9 de la Ley 11/2007, de 22 de junio, sobre transmisión de datos entre Administraciones Públicas, para un eficaz ejercicio del derecho reconocido en su artículo 6.2.b), la Administración General del Estado y sus organismos públicos promoverán la celebración de acuerdos o Convenios con las restantes Administraciones Públicas para facilitar el ejercicio de este derecho por los ciudadanos. En dichos acuerdos o Convenios se establecerán, en particular, los procedimientos que permitan al órgano u organismo cedente comprobar el efectivo ejercicio del derecho respecto de los datos o documentos cuyo acceso hubiera sido solicitado.

TÍTULO II

Sedes electrónicas y punto de acceso general a la Administración General del Estado

Artículo 3. *Creación de la sede electrónica.*

1. Los órganos de la Administración General del Estado y los organismos públicos vinculados o dependientes de la misma crearán sus sedes electrónicas, de acuerdo con los requisitos establecidos en el presente real decreto.

2. Las sedes electrónicas se crearán mediante orden del Ministro correspondiente o resolución del titular del organismo público, que deberá publicarse en el «Boletín Oficial del Estado», con el siguiente contenido mínimo:

a) Ámbito de aplicación de la sede, que podrá ser la totalidad del Ministerio u organismo público, o uno o varios de sus órganos con rango, al menos, de dirección general.

b) Identificación de la dirección electrónica de referencia de la sede.

c) Identificación de su titular, así como del órgano u órganos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos en la misma.

d) 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.

e) Medios disponibles para la formulación de sugerencias y quejas.

f) Cualquier otra circunstancia que se considere conveniente para la correcta identificación de la sede y su fiabilidad.

3. También se podrán crear sedes compartidas mediante orden del Ministro de la Presidencia a propuesta de los Ministros interesados, cuando afecte a varios Departamentos ministeriales, o mediante convenio de colaboración cuando afecte a organismos públicos o cuando intervengan Administraciones autonómicas o locales, que deberá publicarse en el «Boletín Oficial del Estado». Los Convenios de colaboración podrán asimismo determinar la incorporación de un órgano u organismo a una sede preexistente.

Artículo 4. *Características de las sedes electrónicas.*

1. Se realizarán a través de sedes electrónicas todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración Pública o de los ciudadanos por medios electrónicos.

2. Se podrán crear una o varias sedes electrónicas derivadas de una sede electrónica. Las sedes 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.

Las sedes electrónicas derivadas deberán cumplir los mismos requisitos que las sedes electrónicas principales, salvo en lo relativo a la publicación de la orden o resolución por la que se crea, que se realizará a través de la sede de la que dependan. Su ámbito de aplicación comprenderá órgano u órganos con rango, al menos, de subdirección general.

Artículo 5. *Condiciones de identificación de las sedes electrónicas y seguridad de sus comunicaciones.*

1. Las direcciones electrónicas de la Administración General del Estado y de los organismos públicos vinculados o dependientes de la misma que tengan la condición de sedes electrónicas deberán hacerlo constar de forma visible e inequívoca.

2. La sede electrónica tendrá accesible su instrumento de creación, directamente o mediante enlace a su publicación en el «Boletín Oficial del Estado».

3. Las condiciones de identificación de las sedes electrónicas y de seguridad de sus comunicaciones se regirán por lo dispuesto en el título tercero del presente real decreto, y en el título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

4. Los sistemas de información que soporten las sedes electrónicas deberán garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. El Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad establecerán las previsiones necesarias para ello.

Artículo 6. *Contenido y servicios de las sedes electrónicas.*

1. Toda sede electrónica dispondrá del siguiente contenido mínimo:

a) Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión y de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

b) Información necesaria para la correcta utilización de la sede incluyendo el mapa de la sede electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relacionada con propiedad intelectual.

c) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.

d) Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.

e) Relación de sistemas de firma electrónica que, conforme a lo previsto en este real decreto, sean admitidos o utilizados en la sede.

f) Normas de creación del registro o registros electrónicos accesibles desde la sede.

g) 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.

2. Las sedes electrónicas dispondrán de los siguientes servicios a disposición de los ciudadanos:

a) Relación de los servicios disponibles en la sede electrónica.

b) Carta de servicios y carta de servicios electrónicos.

c) Relación de los medios electrónicos a los que se refiere el artículo 27.4 de la Ley 11/2007, de 22 de junio.

d) Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

e) Acceso, en su caso, al estado de tramitación del expediente.

f) En su caso, publicación de los diarios o boletines.

g) En su caso, publicación electrónica de actos y comunicaciones que deban publicarse en tablón de anuncios o edictos, indicando el carácter sustitutivo o complementario de la publicación electrónica.

h) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

i) 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.

j) Indicación de la fecha y hora oficial a los efectos previstos en el artículo 26.1 de la Ley 11/2007, de 22 de junio.

3. Los órganos titulares responsables de la sede podrán además incluir en la misma otros servicios o contenidos, con sujeción a lo previsto en el artículo 10 de la Ley 11/2007, de 22 de junio, y en este real decreto.

4. 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.

5. Las sedes electrónicas cuyo titular tenga competencia sobre territorios con régimen de cooficialidad lingüística posibilitarán el acceso a sus contenidos y servicios en las lenguas correspondientes.

Artículo 7. *Reglas especiales de responsabilidad.*

1. El establecimiento de una sede electrónica conllevará la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma. El titular de la sede electrónica que contenga un enlace o vínculo a otra cuya responsabilidad corresponda a distinto órgano o Administración Pública no será responsable de la integridad, veracidad ni actualización de esta última.

La sede 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.

2. Los órganos u organismos públicos titulares de las sedes electrónicas compartidas previstas en el artículo 3.3 del presente real decreto, responderán, en todo caso, por sus contenidos propios y solidariamente por los contenidos comunes.

Artículo 8. *Directorio de sedes electrónicas.*

1. El Ministerio de la Presidencia gestionará un directorio de sedes electrónicas de la Administración General del Estado y de sus organismos públicos, que será público y accesible desde el punto de acceso general al que se refiere el artículo 9 de este real decreto.

2. En dicho directorio se publicarán las sedes con expresión de su denominación, ámbito de aplicación, titular y la dirección electrónica de las mismas.

Artículo 9. *Punto de acceso general de la Administración General del Estado.*

1. El Punto de acceso general de la Administración General del Estado contendrá la sede electrónica que, en este ámbito, facilita el acceso a los servicios, procedimientos e informaciones accesibles de la Administración General del Estado y de los organismos públicos vinculados o dependientes de la misma. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras Administraciones públicas, mediante la celebración de los correspondientes Convenios.

2. El acceso se organizará atendiendo a distintos criterios que permitan a los ciudadanos identificar de forma fácil e intuitiva los servicios a los que deseen acceder.

3. El Punto de acceso general será gestionado por el Ministerio de la Presidencia, con la participación de todos los Ministerios y, en su caso, de los organismos públicos dotados por la ley de un régimen especial de independencia, para garantizar la completa y exacta incorporación de la información y accesos publicados en éste.

4. El Punto de acceso general podrá incluir servicios adicionales, así como distribuir la información sobre el acceso electrónico a los servicios públicos de manera que pueda ser utilizada por otros departamentos ministeriales, Administraciones o por el sector privado.

TÍTULO III

Identificación y autenticación

CAPÍTULO I

Identificación y autenticación en el acceso electrónico de los ciudadanos a la Administración General del Estado y sus organismos públicos vinculados o dependientes

Artículo 10. *Firma electrónica de los ciudadanos.*

1. Las personas físicas podrán utilizar para relacionarse electrónicamente con la Administración General del Estado y los organismos públicos vinculados o dependientes, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, en todo caso, y los sistemas de firma electrónica avanzada admitidos, a los que se refiere el artículo 13.2.b) de la Ley 11/2007, de 22 de junio.

2. 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 de la Administración General del Estado para los que se admitan.

3. En caso de no admisión, la sede electrónica correspondiente deberá facilitar sistemas alternativos que permitan a las personas jurídicas y a las entidades sin personalidad jurídica el ejercicio de su derecho a relacionarse electrónicamente con la Administración General del Estado.

Artículo 11. *Otros sistemas de firma electrónica.*

1. La admisión de otros sistemas de firma electrónica a la que se refiere el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberán aprobarse mediante orden ministerial, o resolución del titular en el caso de los organismos públicos, previo informe del Consejo Superior de Administración Electrónica.

2. Cuando el sistema se refiera a la totalidad de la Administración General del Estado, se requerirá acuerdo del Consejo de Ministros a propuesta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.

3. El acto de aprobación contendrá la denominación y descripción general del sistema de identificación, órgano u organismo público responsable de su aplicación y garantías de su funcionamiento, y será publicado en las sedes electrónicas que sean de aplicación, donde se

informará de las actuaciones en las que son admisibles estos medios de identificación y autenticación.

Artículo 12. *Disposiciones comunes al 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 que le sea aplicable.

2. El uso por los ciudadanos de sistemas de firma electrónica implicará que los órganos de la Administración General del Estado u organismos públicos vinculados o dependientes pueden tratar los datos personales consignados, a los efectos de la verificación de la firma.

Artículo 13. *Habilitación para la representación de terceros.*

1. De acuerdo con lo previsto en el artículo 23 de la Ley 11/2007, de 22 de junio, la Administración General del Estado y sus organismos públicos vinculados o dependientes podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la presentación electrónica de documentos en representación de los interesados.

La habilitación conllevará la aplicación del régimen de representación regulado en el artículo siguiente.

2. La habilitación requerirá la firma previa de un convenio entre el Ministerio u organismo público competente y la corporación, asociación o institución interesada. El convenio deberá especificar, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables tanto a la persona jurídica o entidad firmante del convenio, como a las personas físicas o jurídicas habilitadas.

Se determinará en cada caso, mediante orden ministerial del Departamento titular de la gestión, los requisitos y condiciones para suscribir los Convenios a que se refiere el presente apartado. Dicha orden deberá garantizar en todo caso el respeto a los principios de objetividad, proporcionalidad y no discriminación en la definición de las condiciones para la habilitación.

3. Los Convenios de habilitación surtirán efectos tanto en relación con la corporación, asociación o institución firmante como con las personas, físicas o jurídicas, que tengan la condición de colegiados, asociados o miembros de aquéllas. Para hacer efectiva la habilitación, éstas últimas deberán suscribir un documento individualizado de adhesión que recoja expresamente la aceptación de su contenido íntegro.

4. El incumplimiento de las obligaciones asumidas por las corporaciones, asociaciones o instituciones firmantes del convenio supondrá su resolución y la de las habilitaciones basadas en el mismo, previa instrucción del oportuno expediente, con audiencia de la entidad interesada.

El incumplimiento por parte de una persona firmante del documento individualizado de adhesión supondrá su exclusión del convenio con el procedimiento y garantías previstos en el párrafo anterior.

En ambos casos se entenderá sin perjuicio de la exigencia de las responsabilidades que fueran procedentes.

Artículo 14. *Régimen de la representación habilitada ante la Administración.*

1. Las personas o entidades habilitadas para la presentación electrónica de documentos en representación de terceros deberán ostentar la representación necesaria para cada actuación, en los términos establecidos en el artículo 32 de la Ley 30/1992, de 26 de noviembre, o en los términos que resulten de la normativa específica de aplicación.

2. La Administración podrá requerir en cualquier momento a las personas habilitadas la acreditación de la representación que ostenten, siendo válida la otorgada a través de los documentos normalizados que apruebe la Administración para cada procedimiento.

La falta de representación suficiente de las personas en cuyo nombre se hubiera presentado la documentación dará lugar a la exigencia de las responsabilidades que fueran procedentes.

3. La habilitación sólo confiere a la persona autorizada la condición de representante para intervenir en los actos expresamente autorizados. No autoriza a recibir ninguna

comunicación de la Administración en nombre del interesado, aun cuando éstas fueran consecuencia del documento presentado.

4. La representación habilitada sólo permite la presentación de solicitudes, escritos o comunicaciones en los registros electrónicos correspondientes al ámbito de la habilitación.

Artículo 15. *Registro electrónico de apoderamientos para actuar electrónicamente ante la Administración General del Estado y sus organismos públicos dependientes o vinculados.*

1. A los efectos exclusivos de la actuación electrónica ante la Administración General del Estado y sus organismos públicos vinculados o dependientes y sin carácter de registro público, se crea, en su ámbito, el registro electrónico de apoderamientos. En él, se podrán hacer constar las representaciones que los interesados otorguen a terceros para actuar en su nombre de forma electrónica ante la Administración General del Estado y/o sus organismos públicos vinculados o dependientes.

2. El Ministerio de la Presidencia creará los ficheros de datos personales necesarios y gestionará dicho registro, que deberá coordinarse con cualquier otro similar existente de ámbito más limitado en la Administración General del Estado.

3. El registro de apoderamientos permitirá a los Ministerios y a los organismos públicos vinculados o dependientes de la Administración General del Estado que se suscriban al mismo, comprobar la representación que ostentan quienes actúen electrónicamente ante ellos en nombre de terceros.

4. Cada Departamento Ministerial y organismo público determinará los trámites y actuaciones de su competencia para los que sea válida la representación incorporada al registro de apoderamientos. Además, caso de entender que hay falta o insuficiencia de la representación formalmente incorporada al registro de apoderamientos podrá requerir al interesado la correspondiente subsanación en los términos del artículo 32.4 de la Ley 30/1992, de 26 de noviembre, o en los términos que resulten de la normativa específica de aplicación.

5. A efectos de su incorporación al registro electrónico de apoderamientos y demás aspectos relativos a su funcionamiento, mediante orden del Ministro de la Presidencia se concretará el régimen de otorgamiento de los apoderamientos, sus formas de acreditación, ámbito de aplicación y revocación de los poderes, así como la forma y lugar de presentación de los documentos acreditativos del poder.

Artículo 16. *Identificación y autenticación de los ciudadanos por funcionario público.*

1. Para llevar a cabo la identificación y autenticación de los ciudadanos por funcionario público conforme a lo previsto en el artículo 22 de la Ley 11/2007, de 22 de junio, en los servicios y procedimientos para los que así se establezca, y en los que resulte necesaria la utilización de sistemas de firma electrónica de los que aquéllos carezcan, se requerirá que el funcionario público habilitado esté dotado de un sistema de firma electrónica admitido por el órgano u organismo público destinatario de la actuación para la que se ha de realizar la identificación o autenticación. El ciudadano, por su parte, habrá de identificarse ante el funcionario y prestar consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

2. El Ministerio de la Presidencia mantendrá actualizado un registro de los funcionarios habilitados en la Administración General del Estado y sus organismos públicos para la identificación y autenticación regulada en este artículo. Mediante el correspondiente Convenio de colaboración podrá extender sus efectos a las relaciones con otras Administraciones públicas.

3. Mediante orden del Ministro de la Presidencia se regulará el funcionamiento del registro de funcionarios habilitados, incluido el sistema para la determinación de los funcionarios que puedan ser habilitados y el alcance de la habilitación.

4. Adicionalmente, los Departamentos Ministeriales y organismos públicos podrán habilitar funcionarios públicos en ellos destinados para identificar y autenticar a ciudadanos ante dicho Departamento ministerial u organismo público.

CAPÍTULO II

Identificación y autenticación de sedes electrónicas y de las comunicaciones que realicen los órganos de la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla

Artículo 17. *Identificación de sedes electrónicas de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.*

1. Las sedes electrónicas se identificarán mediante sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente. Con carácter adicional y para su identificación inmediata, los ciudadanos dispondrán de la información general obligatoria que debe constar en las mismas de acuerdo con lo establecido en el presente real decreto.

2. Para facilitar su identificación, las sedes electrónicas 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 de tercer nivel «.gob.es».

Artículo 18. *Certificados de sede electrónica de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.*

1. Los certificados electrónicos de sede electrónica tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sede electrónica».
b) Nombre descriptivo de la sede electrónica.
c) Denominación del nombre del dominio.
d) Número de identificación fiscal de la entidad suscriptora.
e) Unidad administrativa suscriptora del certificado.

2. El uso de los certificados de sede electrónica está limitado a la identificación de la sede, quedando excluida su aplicación para la firma electrónica de documentos y trámites.

3. El Esquema Nacional de Seguridad, al que se refiere el artículo 42 de la Ley 11/2007, de 22 de junio, determinará las características y requisitos que cumplirán los sistemas de firma electrónica, los certificados y los medios equivalentes que se establezcan en las sedes electrónicas para la identificación y garantía de una comunicación segura.

Artículo 19. *Sistemas de firma electrónica mediante sello electrónico.*

1. La creación de sellos electrónicos se realizará mediante resolución de la Subsecretaría del Ministerio o titular del organismo público competente, que se publicará en la sede 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 General del Estado 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 procedimientos 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 fiscal del suscriptor.

3. El modo de emitir los certificados electrónicos de sello electrónico se definirá en el Esquema Nacional de Seguridad.

Artículo 20. *Sistemas de código seguro de verificación.*

1. La Administración General del Estado y sus organismos públicos vinculados o dependientes podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas. Dicho código vinculará al órgano u organismo y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El carácter único del código generado para cada documento.

b) Su vinculación con el documento generado y con el firmante.

c) Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

3. La aplicación de este sistema requerirá una orden del Ministro competente o resolución del titular del organismo público, previo informe del Consejo Superior de Administración Electrónica, que se publicará en la sede electrónica correspondiente. Dicha orden o resolución del titular del organismo público, además de describir el funcionamiento del sistema, deberá contener de forma inequívoca:

a) Actuaciones automatizadas 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) Indicación de los mecanismos utilizados para la generación del código.

e) Sede electrónica a la que pueden acceder los interesados para la verificación del contenido de la actuación o documento.

f) Plazo de disponibilidad del sistema de verificación respecto a los documentos autorizados mediante este sistema.

4. La Administración responsable de la aplicación de este sistema dispondrá de un procedimiento directo y gratuito para los interesados. El acceso a los documentos originales se realizará de acuerdo con las condiciones y límites que establece la legislación de protección de datos personales u otra legislación específica, así como el régimen general de acceso a la información administrativa establecido en el artículo 37 de la Ley 30/1992, de 26 de noviembre.

5. Se adoptarán las medidas necesarias para garantizar la constancia de la autenticación e integridad de los documentos con posterioridad al vencimiento del plazo de disponibilidad del sistema de verificación, a los efectos de su posterior archivo.

6. Con el fin de mejorar la interoperabilidad electrónica y posibilitar la verificación de la autenticidad de los documentos electrónicos sin necesidad de acceder a la sede electrónica para cotejar el código seguro de verificación, podrá superponerse a éste la firma mediante sello electrónico regulada en el artículo anterior.

Artículo 21. *Firma electrónica mediante medios de autenticación personal.*

El personal al servicio de la Administración General del Estado y de sus organismos públicos vinculados o dependientes utilizará los sistemas de firma electrónica que se determinen en cada caso, entre los siguientes:

a) Firma basada en el Documento Nacional de Identidad electrónico.

b) Firma basada en certificado de empleado público al servicio de la Administración General del Estado expresamente admitidos con esta finalidad.

c) Sistemas de código seguro de verificación, en cuyo caso se aplicará, con las adaptaciones correspondientes, lo dispuesto en el artículo 20.

Artículo 22. *Características de los sistemas de firma electrónica basados en certificados facilitados al personal de la Administración General del Estado o de sus organismos públicos.*

1. Los sistemas de firma electrónica basados en certificados facilitados específicamente a sus empleados por la Administración General del Estado o sus organismos públicos vinculados o dependientes sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan.

2. La firma electrónica regulada en el presente artículo deberá cumplir con las garantías que se establezcan en las políticas de firma que sean aplicables.

3. Los certificados emitidos para la firma, se denominarán «certificado electrónico de empleado público» y tendrán, al menos, el siguiente contenido:

a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público».

b) Nombre y apellidos del titular del certificado.

c) Número del documento nacional de identidad o número de identificación de extranjero del titular del certificado.

d) Órgano u organismo público en el que presta servicios el titular del certificado.

e) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.

CAPÍTULO III

Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad

Artículo 23. *Obligaciones de los prestadores de servicios de certificación.*

1. Los prestadores de servicios de certificación admitidos deberán cumplir las obligaciones de la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como las condiciones generales adicionales a que se refiere el apartado 3.

2. Los prestadores de servicios de certificación deberán facilitar a las plataformas públicas de validación que se establezcan conforme a lo previsto en este real decreto, acceso electrónico y gratuito para la verificación de la vigencia de los certificados asociados a sistemas utilizados por los ciudadanos, la Administración General del Estado y sus organismos públicos.

3. Las condiciones generales adicionales a que se refiere el artículo 4.3 de la Ley 59/2003, de 19 de diciembre, se aprobarán mediante real decreto aprobado por el Consejo de Ministros a propuesta conjunta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.

Corresponde a los Ministerios de la Presidencia y de Industria, Turismo y Comercio publicar la relación de prestadores de servicios de certificación admitidos y de controlar el cumplimiento de las condiciones generales adicionales que se establezcan.

Artículo 24. *Política de firma electrónica y de certificados.*

1. La política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

2. Sin perjuicio de lo dispuesto en el artículo 23, la política de firma electrónica y certificados deberá contener en todo caso:

a) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos.

b) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de certificación asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado recogidas en el presente real decreto.

c) La definición de su ámbito de aplicación.

3. La política de firma electrónica y certificados será aprobada por el Consejo Superior de Administración Electrónica. Mediante resolución del Secretario de Estado para la Función Pública se publicará en el «Boletín Oficial del Estado» el acuerdo de aprobación de la política de firma electrónica y certificados extractado, y de forma íntegra en la sede del Punto de acceso general de la Administración General del Estado.

Artículo 25. *Plataformas de verificación de certificados y sistema nacional de verificación.*

1. El Ministerio de la Presidencia gestionará una plataforma de verificación del estado de revocación de los certificados admitidos en el ámbito de la Administración General del Estado y de los organismos públicos dependientes o vinculados a ella, de acuerdo con lo previsto en el artículo 21.3 de la Ley 11/2007, de 22 de junio. Esta plataforma permitirá verificar el estado de revocación y el contenido de los certificados y prestará el servicio de forma libre y gratuita a todas las Administraciones públicas, españolas o europeas.

2. En el ámbito de sus competencias, los departamentos ministeriales y organismos públicos podrán disponer de sus propias plataformas de verificación del estado de revocación de los certificados.

3. Para mejorar la calidad, robustez y disponibilidad de los servicios de verificación que se ofrecen a todas las Administraciones públicas, se creará el sistema nacional de verificación de certificados compuesto por la Plataforma referida en el apartado uno y aquellas otras que, cumpliendo con lo especificado en el apartado cuatro, se adhieran al mismo. Las plataformas adheridas al sistema nacional podrán delegar operaciones concretas de verificación en cualquiera de ellas. En particular, la operada por el Ministerio de la Presidencia proporcionará servicios de validación de certificados del ámbito europeo al resto de plataformas.

4. Las plataformas de servicios de validación que se integren en el sistema nacional de verificación de certificados deberán cumplir con los siguientes requisitos:

a) Deberán poder obtener y procesar de forma automática las listas de certificados admitidos expedidas de acuerdo con lo establecido en este real decreto y cumplirán con las particularidades que se establezcan en la política de firma y certificados electrónicos que sea de aplicación.

b) Deberán resultar accesibles y prestar sus servicios prioritariamente a través de la red de comunicaciones de las Administraciones Públicas españolas, en las condiciones de seguridad y disponibilidad adecuadas al volumen y la criticidad de los servicios que las usen, pudiendo no obstante contar, como respaldo, con otras vías de acceso.

c) Deberán disponer de documentación y procedimientos operativos del servicio.

d) Deberán garantizar un nivel de servicio que asegure la disponibilidad de la información de estado y validación de certificados en las condiciones que se establezcan en la política de firma y certificados electrónicos.

e) Dispondrán de una declaración de prácticas de validación en la que se detallarán las obligaciones que se comprometen a cumplir en relación con los servicios de verificación. La declaración estará disponible al público por vía electrónica y con carácter gratuito.

f) Deberán habilitar los mecanismos y protocolos de llamada y de sincronización que sean necesarios para crear el sistema nacional de verificación de certificados y acceder a los servicios universales de validación que ofrezca la plataforma operada por el Ministerio de la Presidencia. Basarán su operatividad en las directrices definidas en la política de firma y certificados electrónicos en el ámbito de la Administración General del Estado.

g) Cumplirán lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad respecto de las condiciones generales a las que deberán someterse las plataformas y servicios de validación de certificados.

TÍTULO IV

Registros electrónicos

Artículo 26. *Registros electrónicos.*

Todos los Departamentos Ministeriales de la Administración General del Estado, así como sus organismos públicos, deberán disponer de un servicio de registro electrónico, propio o proporcionado por otro órgano u organismo, para la recepción y remisión de solicitudes, escritos y comunicaciones correspondientes a los procedimientos y actuaciones de su competencia.

Artículo 27. *Creación de registros electrónicos.*

1. La creación de registros electrónicos se efectuará mediante orden del Ministro respectivo o resolución del titular del organismo público, previa aprobación del Ministro de la Presidencia salvo para los organismos públicos en los que no resulte preceptiva, de acuerdo con su normativa específica de organización. Los organismos públicos podrán utilizar los registros electrónicos del departamento ministerial del que dependan, para lo cual suscribirán el correspondiente Convenio.

2. Las disposiciones que creen registros electrónicos contendrán, al menos:

a) Órgano o unidad responsable de la gestión.

b) Fecha y hora oficial y referencia al calendario de días inhábiles que sea aplicable.

c) Identificación del órgano u órganos competentes para la aprobación y modificación de la relación de documentos electrónicos normalizados, que sean del ámbito de competencia del registro, e identificación de los trámites y procedimientos a que se refieren.

d) Medios de presentación de documentación complementaria a una comunicación, escrito o solicitud previamente presentada en el registro electrónico.

3. En ningún caso tendrán la condición de registro electrónico los buzones de correo electrónico corporativo asignado a los empleados públicos o a las distintas unidades y órganos.

4. Tampoco tendrán la consideración de registro electrónico los dispositivos de recepción de fax, salvo aquellos supuestos expresamente previstos en el ordenamiento jurídico.

Artículo 28. *Funciones de los registros electrónicos.*

Los registros electrónicos realizarán las siguientes funciones:

a) La recepción y remisión de solicitudes, escritos y comunicaciones relativas a los trámites y procedimientos que correspondan de acuerdo con su norma de creación, y de los documentos adjuntos, así como la emisión de los recibos necesarios para confirmar la recepción en los términos previstos en el artículo 25 de la Ley 11/2007, de 22 de junio.

b) La remisión electrónica de escritos, solicitudes y comunicaciones a las personas, órganos o unidades destinatarias en los términos del presente real decreto y del artículo 24.2.b) de la Ley 11/2007, de 22 de junio.

c) La anotación de los correspondientes asientos de entrada y salida.

d) Funciones de constancia y certificación en los supuestos de litigios, discrepancias o dudas acerca de la recepción o remisión de solicitudes, escritos y comunicaciones.

Artículo 29. *Solicitudes, escritos y comunicaciones que pueden ser rechazados en los registros electrónicos.*

1. Los registros electrónicos podrán rechazar los documentos electrónicos que se les presenten, en las siguientes circunstancias:

a) Que se trate de documentos dirigidos a órganos u organismos fuera del ámbito de la Administración General del Estado.

b) Que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.

c) En el caso de utilización de documentos normalizados, cuando no se cumplimenten los campos requeridos como obligatorios en la resolución de aprobación del correspondiente documento, o cuando contenga incongruencias u omisiones que impidan su tratamiento.

d) Que se trate de documentos que de acuerdo con lo establecido en los artículos 14 y 32 deban presentarse en registros electrónicos específicos.

2. En los casos previstos en el apartado anterior, se informará de ello al remitente del documento, con indicación de los motivos del rechazo así como, cuando ello fuera posible, de los medios de subsanación de tales deficiencias y dirección en la que pueda presentarse. Cuando el interesado lo solicite se remitirá justificación del intento de presentación, que incluirá las circunstancias de su rechazo.

3. Cuando concurriendo las circunstancias previstas en el apartado 1, no se haya producido el rechazo automático por el registro electrónico, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiendo que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia.

Artículo 30. *Recepción de solicitudes, escritos y comunicaciones.*

1. La presentación de solicitudes, escritos y comunicaciones podrá realizarse en los registros electrónicos durante las veinticuatro horas de todos los días del año.

2. 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.

3. El registro electrónico emitirá automáticamente por el mismo medio un recibo firmado electrónicamente, mediante alguno de los sistemas de firma del artículo 18 de la Ley 11/2007, de 22 de junio, con el siguiente contenido:

a) Copia del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.

b) Fecha y hora de presentación y número de entrada de registro.

c) En su caso, enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.

d) Información del plazo máximo establecido normativamente para la resolución y notificación del procedimiento, así como de los efectos que pueda producir el silencio administrativo, cuando sea automáticamente determinable.

Artículo 31. *Creación, naturaleza y funcionamiento del Registro Electrónico Común.*

1. Se crea el Registro Electrónico Común de la Administración General del Estado, accesible a través del punto de acceso general establecido en el artículo 9.

2. El Registro Electrónico Común será gestionado por el Ministerio de la Presidencia.

3. El Registro Electrónico Común posibilitará la presentación de cualesquiera solicitudes, escritos y comunicaciones dirigidas a la Administración General del Estado y a sus organismos públicos.

4. El Registro Electrónico Común informará al ciudadano y le redirigirá, cuando proceda, a los registros competentes para la recepción de aquellos documentos que dispongan de aplicaciones específicas para su tratamiento.

5. Mediante orden del Ministro de la Presidencia se establecerán los requisitos y condiciones de funcionamiento del Registro Electrónico Común, incluyendo la creación de un

fichero ajustado a las previsiones de la normativa sobre protección de datos de carácter personal, así como los demás aspectos previstos en el artículo 27.2.

TÍTULO V

De las comunicaciones y las notificaciones

CAPÍTULO I

Comunicaciones electrónicas

Artículo 32. *Obligatoriedad de la comunicación a través de medios electrónicos.*

1. La obligatoriedad de comunicarse por medios electrónicos con los órganos de la Administración General del Estado o sus organismos públicos vinculados o dependientes, en los supuestos previstos en el artículo 27.6 de la Ley 11/2007, de 22 de junio, podrá establecerse mediante orden ministerial. Esta obligación puede comprender, en su caso, la práctica de notificaciones administrativas por medios electrónicos, así como la necesaria utilización de los registros electrónicos que se especifiquen.

2. En la norma que establezca dicha obligación se especificarán las comunicaciones a las que se aplique, el medio electrónico de que se trate y los sujetos obligados. Dicha orden deberá ser publicada en el «Boletín Oficial del Estado» y en la sede electrónica del órgano u organismo público de que se trate.

3. Si existe la obligación de comunicación a través de medios electrónicos y no se utilizan dichos medios, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiendo que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia.

Artículo 33. *Modificación del medio de comunicación inicialmente elegido.*

Salvo las excepciones previstas en el artículo anterior, los ciudadanos podrán modificar la manera de comunicarse con los órganos u organismos públicos vinculados o dependientes de la Administración General del Estado, optando por un medio distinto del inicialmente elegido, que comenzará a producir efectos respecto de las comunicaciones que se produzcan a partir del día siguiente a su recepción en el registro del órgano competente.

Artículo 34. *Comunicaciones entre los órganos de la Administración General del Estado y sus organismos públicos.*

1. Los órganos de la Administración General del Estado y sus organismos públicos deberán utilizar medios electrónicos para comunicarse entre ellos. Sólo con carácter excepcional se podrán utilizar otros medios de comunicación cuando no sea posible la utilización de medios electrónicos por causas justificadas de carácter técnico.

2. Los órganos de la Administración General del Estado y sus organismos públicos deberán utilizar medios electrónicos para comunicarse con otras Administraciones públicas. No obstante, se podrán utilizar otros medios de comunicación atendiendo a los medios técnicos de que éstas dispongan.

Se suscribirán los Convenios necesarios para garantizar las condiciones de dicha comunicación, salvo cuando dichas condiciones se encuentren reguladas en normas específicas.

CAPÍTULO II

Notificaciones electrónicas

Artículo 35. *Práctica de notificaciones por medios electrónicos.*

1. Los órganos y organismos públicos de la Administración General del Estado habilitarán sistemas de notificación electrónica de acuerdo con lo dispuesto en el presente capítulo.

2. La práctica de notificaciones por medios electrónicos podrá efectuarse, de alguna de las formas siguientes:

a) Mediante la dirección electrónica habilitada en la forma regulada en el artículo 38 de este real decreto.

b) Mediante sistemas de correo electrónico con acuse de recibo que deje constancia de la recepción en la forma regulada en el artículo 39 de este real decreto.

c) Mediante comparecencia electrónica en la sede en la forma regulada en el artículo 40 de este real decreto.

d) Otros medios de notificación electrónica que puedan establecerse, siempre que quede constancia de la recepción por el interesado en el plazo y en las condiciones que se establezcan en su regulación específica.

Artículo 36. *Elección del medio de notificación.*

1. Las notificaciones se efectuarán por medios electrónicos cuando así haya sido solicitado o consentido expresamente por el interesado o cuando haya sido establecida como obligatoria conforme a lo dispuesto en los artículos 27.6 y 28.1 de la Ley 11/2007, de 22 de junio.

2. La solicitud deberá manifestar la voluntad de recibir las notificaciones por alguna de las formas electrónicas reconocidas, e indicar un medio de notificación electrónica válido conforme a lo establecido en el presente real decreto.

3. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento podrán emitirse y recabarse, en todo caso, por medios electrónicos.

4. Cuando la notificación deba admitirse obligatoriamente por medios electrónicos, el interesado podrá elegir entre las distintas formas disponibles salvo que la normativa que establece la notificación electrónica obligatoria señale una forma específica.

5. Cuando, como consecuencia de la utilización de distintos medios, electrónicos o no electrónicos, se practiquen varias notificaciones de un mismo acto administrativo, se entenderán producidos todos los efectos jurídicos derivados de la notificación, incluido el inicio del plazo para la interposición de los recursos que procedan, a partir de la primera de las notificaciones correctamente practicada. Las Administraciones públicas podrán advertirlo de este modo en el contenido de la propia notificación.

6. Se entenderá consentida la práctica de la notificación por medios electrónicos respecto de una determinada actuación administrativa cuando, tras haber sido realizada por una de las formas válidamente reconocidas para ello, el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación. La notificación surtirá efecto a partir de la fecha en que el interesado realice dichas actuaciones.

En el supuesto previsto en el párrafo anterior, el resto de las resoluciones o actos del procedimiento deberán notificarse por el medio y en la forma que proceda conforme a lo dispuesto en la Ley 11/2007, de 22 de junio, y en el presente real decreto.

Artículo 37. *Modificación del medio de notificación.*

1. Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, de 26 de noviembre, excepto en los casos en que la notificación por medios electrónicos tenga

carácter obligatorio conforme a lo dispuesto en los artículos 27.6 y 28.1 de la Ley 11/2007, de 22 de junio.

2. En la solicitud de modificación del medio de notificación preferente deberá indicarse el medio y lugar para la práctica de las notificaciones posteriores.

3. El cambio de medio a efectos de las notificaciones se hará efectivo para aquellas notificaciones que se emitan desde el día siguiente a la recepción de la solicitud de modificación en el registro del órgano u organismo público actuante.

Artículo 38. *Notificación mediante la puesta a disposición del documento electrónico a través de dirección electrónica habilitada.*

1. Serán válidos los sistemas de notificación electrónica a través de dirección electrónica habilitada siempre que cumplan, al menos, los siguientes requisitos:

a) Acreditar la fecha y hora en que se produce la puesta a disposición del interesado del acto objeto de notificación.

b) Posibilitar el acceso permanente de los interesados a la dirección electrónica correspondiente, a través de una sede electrónica o de cualquier otro modo.

c) Acreditar la fecha y hora de acceso a su contenido.

d) Poseer mecanismos de autenticación para garantizar la exclusividad de su uso y la identidad del usuario.

2. Bajo responsabilidad del Ministerio de la Presidencia existirá un sistema de dirección electrónica habilitada para la práctica de estas notificaciones que quedará a disposición de todos los órganos y organismos públicos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios. Los ciudadanos podrán solicitar la apertura de esta dirección electrónica, que tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará ésta dirección electrónica, comunicándose así al interesado.

3. Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada a que se refiere el apartado anterior será asignada de oficio y podrá tener vigencia indefinida, conforme al régimen que se establezca por la orden del Ministro de la Presidencia a la que se refiere la disposición final primera. Respecto del resto de direcciones electrónicas habilitadas dicho régimen se establecerá mediante orden del titular del Departamento correspondiente.

Artículo 39. *Notificación mediante recepción en dirección de correo electrónico.*

Se podrá acordar la práctica de notificaciones en las direcciones de correo electrónico que los ciudadanos elijan siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento del acceso al contenido de la notificación.

Artículo 40. *Notificación por comparecencia electrónica.*

1. La notificación por comparecencia electrónica consiste en el acceso por el interesado, debidamente identificado, al contenido de la actuación administrativa correspondiente a través de la sede electrónica del órgano u organismo público actuante.

2. Para que la comparecencia electrónica produzca los efectos de notificación de acuerdo con el artículo 28.5 de la Ley 11/2007, de 22 de junio, se requerirá que reúna las siguientes condiciones:

a) Con carácter previo al acceso a su contenido, el interesado deberá visualizar un aviso del carácter de notificación de la actuación administrativa que tendrá dicho acceso.

b) El sistema de información correspondiente dejará constancia de dicho acceso con indicación de fecha y hora.

TÍTULO VI

Los documentos electrónicos y sus copias

CAPÍTULO I

Disposiciones comunes sobre los documentos electrónicos

Artículo 41. *Características del documento electrónico.*

1. Los documentos electrónicos deberán cumplir los siguientes requisitos para su validez:

a) Contener información de cualquier naturaleza.

b) Estar archivada la información en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

c) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

2. Los documentos administrativos electrónicos deberán, además de cumplir las anteriores condiciones, haber sido expedidos y firmados electrónicamente mediante los sistemas de firma previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y ajustarse a los requisitos de validez previstos en la Ley 30/1992, de 26 de noviembre.

Artículo 42. *Adición de metadatos a los documentos electrónicos.*

1. Se entiende como metadato, a los efectos de este real decreto, cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento.

2. Los documentos electrónicos susceptibles de ser integrados en un expediente electrónico, deberán tener asociados metadatos que permitan su contextualización en el marco del órgano u organismo, la función y el procedimiento administrativo al que corresponde.

Además, se asociará a los documentos electrónicos la información relativa a la firma del documento así como la referencia temporal de los mismos, en la forma regulada en el presente real decreto.

3. La asociación de metadatos a los documentos electrónicos aportados por los ciudadanos o emitidos por la Administración General del Estado o sus organismos públicos será, en todo caso, realizada por el órgano u organismo actuante, en la forma que en cada caso se determine.

4. Los metadatos mínimos obligatorios asociados a los documentos electrónicos, así como la asociación de los datos de firma o de referencia temporal de los mismos, se especificarán en el Esquema Nacional de Interoperabilidad.

5. Una vez asociados los metadatos a un documento electrónico, no podrán ser modificados en ninguna fase posterior del procedimiento administrativo, con las siguientes excepciones:

a) Cuando se observe la existencia de errores u omisiones en los metadatos inicialmente asignados.

b) Cuando se trate de metadatos que requieran actualización, si así lo dispone el Esquema Nacional de Interoperabilidad.

La modificación de los metadatos deberá ser realizada por el órgano competente conforme a la normativa de organización específica, o de forma automatizada conforme a las normas que se establezcan al efecto.

6. Independientemente de los metadatos mínimos obligatorios a que se refiere el apartado 4, los distintos órganos u organismos podrán asociar a los documentos electrónicos

metadatos de carácter complementario, para las necesidades de catalogación específicas de su respectivo ámbito de gestión, realizando su inserción de acuerdo con las especificaciones que establezca al respecto el Esquema Nacional de Interoperabilidad. Los metadatos complementarios no estarán sujetos a las prohibiciones de modificación establecidas en el apartado anterior.

Artículo 43. *Copias electrónicas de los documentos electrónicos realizadas por la Administración General del Estado y sus organismos públicos.*

1. Las copias electrónicas generadas que, por ser idénticas al documento electrónico original no comportan cambio de formato ni de contenido, tendrán la eficacia jurídica de documento electrónico original.

2. En caso de cambio del formato original, para que una copia electrónica de un documento electrónico tenga la condición de copia auténtica, deberán cumplirse los siguientes requisitos:

a) Que el documento electrónico original, que debe conservarse en todo caso, se encuentre en poder de la Administración.

b) Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

c) Que incluya su carácter de copia entre los metadatos asociados.

d) Que sea autorizada mediante firma electrónica conforme a los sistemas recogidos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

3. Se podrán generar copias electrónicas auténticas a partir de otras copias electrónicas auténticas siempre que se observen los requisitos establecidos en los apartados anteriores.

4. Los órganos emisores de los documentos administrativos electrónicos o receptores de los documentos privados electrónicos, o los archivos que reciban los mismos, están obligados a la conservación de los documentos originales, aunque se hubiere procedido a su copiado conforme a lo establecido en el presente artículo, sin perjuicio de lo previsto en el artículo 52.

5. Será considerada copia electrónica auténtica de documentos electrónicos presentados conforme a sistemas normalizados o formularios:

a) La obtenida conforme a lo señalado en los apartados anteriores de este artículo.

b) El documento electrónico, autenticado con la firma electrónica del órgano u organismo destinatario, resultado de integrar el contenido variable firmado y remitido por el ciudadano en el formulario correspondiente empleado en la presentación.

Artículo 44. *Copias electrónicas de documentos en soporte no electrónico.*

1. Las copias electrónicas de los documentos en soporte papel o en otro soporte susceptible de digitalización realizadas por la Administración General del Estado y sus organismos públicos vinculados o dependientes, ya se trate de documentos emitidos por la Administración o documentos privados aportados por los ciudadanos, se realizarán de acuerdo con lo regulado en el presente artículo.

2. A los efectos de lo regulado en este real decreto, se define como «imagen electrónica» el resultado de aplicar un proceso de digitalización a un documento en soporte papel o en otro soporte que permita la obtención fiel de dicha imagen.

Se entiende por «digitalización» el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra, del documento.

3. Cuando sean realizadas por la Administración, las imágenes electrónicas tendrán la naturaleza de copias electrónicas auténticas, con el alcance y efectos previstos en el artículo 46 de la Ley 30/1992, de 26 de noviembre, siempre que se cumplan los siguientes requisitos:

a) Que el documento copiado sea un original o una copia auténtica.

b) Que la copia electrónica sea autorizada mediante firma electrónica utilizando los sistemas recogidos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

c) Que las imágenes electrónicas estén codificadas conforme a alguno de los formatos y con los niveles de calidad y condiciones técnicas especificados en el Esquema Nacional de Interoperabilidad.

d) Que la copia electrónica incluya su carácter de copia entre los metadatos asociados.

e) Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

4. No será necesaria la intervención del órgano administrativo depositario del documento administrativo original para la obtención de copias electrónicas auténticas, cuando las imágenes electrónicas sean obtenidas a partir de copias auténticas en papel emitidas cumpliendo los requisitos del artículo 46 de la Ley 30/1992, de 26 de noviembre.

Artículo 45. *Copias en papel de los documentos públicos administrativos electrónicos realizadas por la Administración General del Estado y sus organismos públicos vinculados o dependientes.*

Para que las copias emitidas en papel de los documentos públicos administrativos electrónicos tengan la consideración de copias auténticas deberán cumplirse los siguientes requisitos:

a) Que el documento electrónico copiado sea un documento original o una copia electrónica auténtica del documento electrónico o en soporte papel original, emitidos conforme a lo previsto en el presente real decreto.

b) La impresión en el mismo documento de un código generado electrónicamente u otro sistema de verificación, con indicación de que el mismo permite contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u organismo público emisor.

c) Que la copia sea obtenida conforme a las normas de competencia y procedimiento, que en cada caso se aprueben, incluidas las de obtención automatizada.

Artículo 46. *Destrucción de documentos en soporte no electrónico.*

1. Los documentos originales y las copias auténticas en papel o cualquier otro soporte no electrónico admitido por la ley como prueba, de los que se hayan generado copias electrónicas auténticas, podrán destruirse en los términos y condiciones que se determinen en las correspondientes Resoluciones, si se cumplen los siguientes requisitos:

a) La destrucción requerirá una resolución adoptada por el órgano responsable del procedimiento o, en su caso, por el órgano responsable de la custodia de los documentos, previo el oportuno expediente de eliminación, en el que se determinen la naturaleza específica de los documentos susceptibles de destrucción, los procedimientos administrativos afectados, las condiciones y garantías del proceso de destrucción, y la especificación de las personas u órganos responsables del proceso.

Las resoluciones que aprueben los procesos de destrucción regulados en el artículo 30.4 de la Ley 11/2007, de 22 de junio, requerirán informe previo de la respectiva Comisión Calificadora de Documentos Administrativos y posterior dictamen favorable de la Comisión Superior Calificadora de Documentos Administrativos, sin que, en su conjunto, este trámite de informe pueda ser superior a tres meses. Una vez superado este plazo sin pronunciamiento expreso de ambos órganos, podrá resolverse el expediente de eliminación y procederse a la destrucción.

b) Que no se trate de documentos con valor histórico, artístico o de otro carácter relevante que aconseje su conservación y protección, o en el que figuren firmas u otras expresiones manuscritas o mecánicas que confieran al documento un valor especial.

2. Se deberá incorporar al expediente de eliminación un análisis de los riesgos relativos al supuesto de destrucción de que se trate, con mención explícita 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.

3. La destrucción de cualquier tipo de documento diferente de los previstos en los apartados anteriores, se regirá por lo previsto 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 la conservación de documentos administrativos en soporte distinto al original.

CAPÍTULO II

Normas específicas relativas a los documentos administrativos electrónicos

Artículo 47. *Referencia temporal de los documentos administrativos electrónicos.*

1. La Administración General del Estado y sus organismos públicos dependientes o vinculados asociarán a los documentos administrativos electrónicos, en los términos del artículo 29.2 de la Ley 11/2007, de 22 de junio, 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. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.

b) «Sello 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 de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

La información relativa a las marcas y sellos de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad.

2. La relación de prestadores de servicios de certificación electrónica que prestan servicios de sellado de tiempo en la Administración General del Estado, conforme a lo dispuesto en el artículo 29.3 de la Ley 11/2007, de 22 de junio, así como los requisitos que han de cumplirse para dicha admisión, serán regulados mediante el real decreto a que se refiere el artículo 23.3.

CAPÍTULO III

Normas específicas relativas a los documentos electrónicos aportados por los ciudadanos

Artículo 48. *Imágenes electrónicas aportadas por los ciudadanos.*

1. De conformidad con el artículo 35.2 de la Ley 11/2007, de 22 de junio, los interesados podrán aportar al expediente, en cualquier fase del procedimiento, copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos. Las mencionadas imágenes electrónicas carecerán del carácter de copia auténtica.

2. Las imágenes electrónicas presentadas por los ciudadanos deberán ajustarse a los formatos y estándares aprobados para tales procesos en el Esquema Nacional de Interoperabilidad. En caso de incumplimiento de este requisito, se requerirá al interesado para la subsanación del defecto advertido, en los términos establecidos en el artículo 71 de la Ley 30/1992, de 26 de noviembre.

3. La presentación documental que realicen los interesados en cualquiera de los lugares de presentación establecidos en el artículo 2.1.a), b) y d) del Real Decreto 772/1999, de 7 de mayo, podrá acompañarse de soportes conteniendo documentos electrónicos con los efectos establecidos en el artículo 35.2 de la Ley 11/2007, de 22 de junio.

4. Será de aplicación a las solicitudes de cotejo de las copias aportadas, previstas en el artículo 35.2 de la Ley 11/2007, de 22 de junio, lo establecido en relación con la transmisión de datos en el artículo 2 del presente real decreto.

CAPÍTULO IV

Normas relativas a la obtención de copias electrónicas por los ciudadanos

Artículo 49. *Obtención de copias electrónicas de documentos electrónicos.*

Los ciudadanos podrán ejercer el derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan condición de interesados de acuerdo con lo dispuesto en la normativa reguladora del respectivo procedimiento.

La obtención de la copia podrá realizarse mediante extractos de los documentos o se podrá utilizar otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

Artículo 50. *Obtención de copias electrónicas a efectos de compulsa.*

Cuando los interesados deseen ejercer el derecho regulado en el artículo 8.1 del Real Decreto 772/1999, de 7 de mayo, sobre aportación de copias compulsadas al procedimiento, y siempre que los originales no deban obrar en el procedimiento, la oficina receptora, si cuenta con los medios necesarios, deberá proceder a la obtención de copia electrónica de los documentos a compulsar mediante el procedimiento regulado en el artículo 44 de este real decreto, siempre que se trate de uno de los lugares de presentación mencionados en el artículo 2.1.a), b) y d) del citado real decreto.

Estas copias digitalizadas serán firmadas electrónicamente mediante los procedimientos previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y tendrán el carácter de copia compulsada o cotejada previsto en el artículo 8 del Real Decreto 772/1999, de 7 de mayo, sin que en ningún caso se acredite la autenticidad del documento original, no siéndoles de aplicación el procedimiento de comprobación previsto en el artículo 35.2 de dicha ley.

CAPÍTULO V

Archivo electrónico de documentos

Artículo 51. *Archivo electrónico de documentos.*

1. La Administración General del Estado y sus organismos públicos vinculados o dependientes deberán conservar en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas, que formen parte de un expediente administrativo, así como aquellos otros que, tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.

2. La conservación de los documentos electrónicos podrá realizarse bien de forma unitaria, o mediante 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 firma electrónica de dichos datos.

Artículo 52. *Conservación de documentos electrónicos.*

1. Los períodos mínimos de conservación de los documentos electrónicos se determinarán por cada órgano administrativo de acuerdo con el procedimiento administrativo de que se trate, siendo en todo caso de aplicación, con la excepción regulada de la destrucción de documentos en papel copiados electrónicamente, las normas generales sobre conservación del patrimonio documental con valor histórico y sobre eliminación de documentos de la Administración General del Estado y sus organismos públicos.

2. Para preservar la conservación, el acceso y la legibilidad de los documentos electrónicos archivados, podrán realizarse operaciones de conversión, de acuerdo con las normas sobre copiado de dichos documentos contenidas en el presente real decreto.

3. Los responsables de los archivos electrónicos promoverán el copiado auténtico con cambio de formato de los documentos y expedientes del archivo tan pronto como el formato de los mismos deje de figurar entre los admitidos en la gestión pública por el Esquema Nacional de Interoperabilidad.

CAPÍTULO VI

Expediente electrónico

Artículo 53. *Formación del expediente electrónico.*

1. La formación de los expedientes electrónicos es responsabilidad del órgano que disponga la normativa de organización específica y, de no existir previsión normativa, del encargado de su tramitación.

2. Los expedientes electrónicos que deban ser objeto de remisión o puesta a disposición se formarán ajustándose a las siguientes reglas:

a) Los expedientes electrónicos dispondrán de un código que permita su identificación unívoca por cualquier órgano de la Administración en un entorno de intercambio interadministrativo.

b) El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado electrónicamente mediante los sistemas previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y en los términos del artículo 32.2 de la citada ley.

c) Con el fin de garantizar la interoperabilidad de los expedientes, tanto su estructura y formato como las especificaciones de los servicios de remisión y puesta a disposición se sujetarán a lo que se establezca al respecto por el Esquema Nacional de Interoperabilidad.

d) Los expedientes electrónicos estarán integrados por documentos electrónicos, que podrán formar parte de distintos expedientes, pudiendo incluir asimismo otros expedientes electrónicos si así lo requiere el procedimiento. Excepcionalmente, cuando la naturaleza o la extensión de determinados documentos a incorporar al expediente no permitan o dificulten notablemente su inclusión en el mismo conforme a los estándares y procedimientos establecidos, deberán incorporarse al índice del expediente sin perjuicio de su aportación separada.

e) Los documentos que se integran en el expediente electrónico se ajustarán al formato o formatos de larga duración, accesibles en los términos que determine el Esquema Nacional de Interoperabilidad.

Disposición adicional primera. *Procedimientos especiales.*

1. Lo dispuesto en este real decreto se entiende sin perjuicio de la regulación especial contenida en la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público y sus normas de desarrollo en relación con el perfil del contratante, Plataforma de Contratación del Estado y uso de medios electrónicos en los procedimientos relacionados con la contratación pública.

2. La aplicación de las disposiciones de este real decreto sobre gestión electrónica de procedimientos en materia tributaria, de seguridad social y desempleo y de régimen jurídico de los extranjeros en España, se efectuará de conformidad con lo establecido en las disposiciones adicionales quinta, sexta, séptima y decimonovena de la Ley 30/1992, de 26 de noviembre.

3. Lo dispuesto en el presente real decreto se aplicará supletoriamente al régimen especial previsto en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido y en la Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas contenidas en el citado real decreto. Este régimen

jurídico especial será aplicable a cualesquiera copias electrónicas de facturas que deban remitirse a los órganos y organismos de la Administración General del Estado.

4. Lo dispuesto en este real decreto se entiende sin perjuicio de la regulación contenida en los reales decretos 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado» y 1979/2008, de 28 de noviembre, por el que se regula la edición electrónica del «Boletín Oficial del Registro Mercantil».

Disposición adicional segunda. *Función estadística.*

Lo dispuesto en el artículo 2 no se aplicará a la recogida de datos prevista en el Capítulo II de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

Disposición adicional tercera. *Directorio de sedes electrónicas.*

En el plazo de 6 meses, contados a partir de la entrada en vigor de este real decreto, el Ministerio de la Presidencia publicará en su sede electrónica el Directorio de sedes electrónicas a que se refiere el artículo 8.

Disposición adicional cuarta. *Conservación de la identificación de direcciones electrónicas.*

Sin perjuicio de lo establecido, con carácter general, en el artículo 17.2, las direcciones electrónicas actualmente existentes de los organismos públicos que gocen de un alto nivel de conocimiento público, podrán ser mantenidas con la misma identificación electrónica.

Disposición adicional quinta. *Plataforma de verificación de certificados de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

De conformidad con las facultades que otorga a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social en relación con la disposición adicional cuarta de la Ley 59/2003, de 19 de diciembre, de firma electrónica, la plataforma de verificación de certificados desarrollada por esta entidad se integrará en el sistema nacional de verificación de certificados regulado en el artículo 25.3 del presente real decreto, cumpliendo con lo especificado en el artículo 25.4.

El Ministerio de la Presidencia y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda adoptarán las medidas para conseguir la permanente y perfecta coordinación operativa y la coherencia técnica de ambas plataformas de verificación, con la finalidad de asegurar su interoperabilidad y garantizar el mejor servicio a las Administraciones y los ciudadanos.

Disposición adicional sexta. *Ausencia de impacto presupuestario.*

La aplicación de las previsiones contenidas en este real decreto no deberá ocasionar incremento del gasto público ni disminución de los ingresos públicos. Por tanto, los departamentos ministeriales afectados deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

Disposición transitoria primera. *Sistemas de firma electrónica.*

1. En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad podrán seguir utilizándose los medios actualmente admitidos de identificación y autenticación. Dichos esquemas establecerán los plazos de aprobación de las relaciones de medios admitidos así como los plazos máximos de utilización de los medios que habiendo sido utilizados no se adecúen a las prescripciones de los mismos.

2. En particular, podrá seguir utilizándose para los usos previstos en este real decreto y con los mismos efectos jurídicos que el sello electrónico, la firma electrónica de persona jurídica o del titular del órgano administrativo con observancia de lo dispuesto en la normativa correspondiente.

Disposición transitoria segunda. *Condiciones de seguridad de las plataformas de verificación.*

En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad, seguirán teniendo validez los sistemas y servicios de verificación existentes y operativos a la entrada en vigor de este real decreto. Los certificados vinculados a dichos sistemas o servicios podrán utilizarse en los procedimientos que expresamente los prevean.

Disposición transitoria tercera. *Sistema de notificación electrónica regulado en el artículo 38.2.*

Mientras no se proceda a dictar la regulación del Sistema de notificación electrónica regulado en el artículo 38.2, de acuerdo con la disposición final primera, la función prevista en el sistema de notificación se realizará a través de los servicios autorizados, de conformidad con la Orden PRE 1551/2003, de 10 junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por la que se regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

Disposición transitoria cuarta. *Adaptación de sedes electrónicas.*

En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad, la creación de sedes deberá ir acompañada de un informe en el que se acredite el cumplimiento de las condiciones de confidencialidad, disponibilidad e integridad de las informaciones y comunicaciones que se realicen a través de las mismas.

Disposición transitoria quinta. *Adaptación en la Administración General del Estado en el Exterior.*

La aplicación de lo dispuesto en este real decreto a la Administración General del Estado en el Exterior se efectuará según los medios de identificación y autenticación de los ciudadanos, los canales electrónicos y condiciones de funcionamiento que en cada momento se encuentren disponibles.

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 especialmente:

a) El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

b) Los artículos 14 a 18 del Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

Disposición final primera. *Sistema de notificación electrónica regulado en el artículo 38.2.*

Por orden del Ministro de la Presidencia se establecerá el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2, que deberá ajustarse a las previsiones del mismo.

Disposición final segunda. *Punto de acceso general.*

En el plazo de 3 meses desde la entrada en vigor de este real decreto, el Ministro de la Presidencia dictará las disposiciones necesarias para la constitución del punto de acceso general de la Administración General del Estado regulado en el artículo 9.

Disposición final tercera. *Registros electrónicos.*

Los registros telemáticos existentes a la entrada en vigor de la Ley 11/2007, de 22 de junio, afectados por el apartado 2 de la disposición transitoria única de la citada ley,

ajustarán su funcionamiento a lo establecido en este real decreto dentro de los seis meses siguientes a su entrada en vigor.

La adaptación a lo dispuesto en el presente real decreto se realizará mediante orden ministerial o, en su caso, resolución del titular del correspondiente organismo público, por la que se explicite el cumplimiento de lo dispuesto en el artículo 27.

Disposición final cuarta. *Sedes electrónicas.*

Los puntos de acceso electrónico pertenecientes a la Administración General del Estado o sus organismos públicos dependientes o vinculados en los que se desarrollan actualmente comunicaciones con terceros, propias de sede electrónica, deberán adaptarse, en el plazo de cuatro meses, contados a partir de la entrada en vigor de este real decreto, a lo dispuesto en el mismo para las sedes o, en su caso, subsedes, electrónicas, sin perjuicio de lo previsto en las disposiciones transitorias primera y segunda de este real decreto y en la disposición final tercera.2 de la Ley 11/2007, de 22 de junio.

Disposición final quinta. *Habilitación para el desarrollo normativo.*

Se habilita a los Ministros de la Presidencia, Economía y Hacienda e Industria, Turismo y Comercio para dictar las disposiciones que sean necesarias para el desarrollo de este real decreto, en el ámbito de sus respectivas competencias.

Disposición final sexta. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 3

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: sin modificaciones
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 será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a 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 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.*

1. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por las Administraciones públicas se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

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.

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 sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.

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 registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán 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.

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. *Guías de seguridad.*

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.

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 articulará los procedimientos necesarios para conocer regularmente 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.

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.

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 los informes de auditoría de los sistemas afectados.

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. *Instituto Nacional de Tecnologías de la Comunicación (INTECO) y organismos análogos.*

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), como centro de excelencia promovido por el Ministerio de Industria, Turismo y Comercio para el desarrollo de la sociedad del conocimiento, podrá desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas en el presente real decreto.

Asimismo, las Administraciones públicas podrán disponer de entidades análogas para llevar a cabo dichas actividades u otras adicionales en el ámbito de sus competencias.

Disposición adicional tercera. *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 cuarta. *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 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

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				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
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 incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
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

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				op	Marco operacional
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				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	n.a.	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

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				mp	Medidas de protección
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	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
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.

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:

a) Documentación de las instalaciones:

1.º Áreas.
2.º Puntos de acceso.

b) Documentación del sistema:

1.º Equipos.
2.º Redes internas y conexiones al exterior.
3.º Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c) Esquema de líneas de defensa:

1.º Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet.
2.º Cortafuegos, DMZ, etc.
3.º Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

d) Sistema de identificación y autenticación de usuarios:

1.º Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.

2.º Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

e) Controles técnicos internos:

1.º Validación de datos de entrada, salida y datos intermedios.

f) Sistema de gestión con actualización y aprobación periódica.

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 preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y que estén certificados por entidades independientes de reconocida solvencia.
Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.
Tendrán la consideración de entidades independientes de reconocida solvencia las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información u otras de naturaleza análoga.

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:

a) Se asignará un identificador singular para cada entidad (usuario o proceso) que accede al sistema, de tal forma que:

1.º Se puede saber quién recibe y qué derechos de acceso recibe.
2.º Se puede saber quién ha hecho algo y qué ha hecho.

b) Las cuentas de usuario se gestionarán de la siguiente forma:

1.º Cada cuenta estará asociada a un identificador único.
2.º 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.
3.º 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.

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	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados a cada nivel.

Nivel BAJO

a) Se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, o dispositivos físicos (en expresión inglesa »tokens») o componentes lógicos tales como certificados software u otros equivalentes o mecanismos biométricos.

b) En el caso de usar contraseñas se aplicarán reglas básicas de calidad de las mismas.
c) Se atenderá a la seguridad de los autenticadores de forma que:

1.º Los autenticadores se activarán una vez estén bajo el control efectivo del usuario.
2.º Los autenticadores estarán bajo el control exclusivo del usuario.
3.º El usuario reconocerá que los 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.º Los autenticadores se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5.º Los autenticadores se retirarán y serán deshabilitados cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) No se recomendará el uso de claves concertadas.
b) Se recomendará el uso de otro tipo de mecanismos del tipo dispositivos físicos (tokens) o componentes lógicos tales como certificados software u otros equivalentes o biométricos.
c) En el caso de usar contraseñas se aplicarán políticas rigurosas de calidad de la contraseña y renovación frecuente.

Nivel ALTO

a) Los autenticadores se suspenderán tras un periodo definido de no utilización.
b) No se admitirá el uso de claves concertadas.
c) Se exigirá el uso de dispositivos físicos (tokens) personalizados o biometría.
d) En el caso de utilización de dispositivos físicos (tokens) se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
e) Se emplearán, preferentemente, productos certificados [op.pl.5].

Tabla resumen de mecanismos de autenticación admisibles

		Nivel		
		BAJO	MEDIO	ALTO
algo que se sabe	claves concertadas	sí	Con cautela	no
algo que se tiene	Tokens	si	sí	criptográficos
algo que se es	Biometría	sí	sí	+ doble factor

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 incidencias (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 incidencias [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 incidentes reales o sospechosos, detallando 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.º Prevenir que se repita el incidente.

2.º Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

3.º Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.

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
	no aplica	no aplica	aplica

Nivel ALTO

Se registrarán todas las actividades de los usuarios en el sistema, de forma que:

a) El registro indicará quién realiza la actividad, cuando la realiza y sobre qué información.
b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.
c) Deben registrarse las actividades realizadas con éxito y los intentos fracasados.
d) La determinación de qué actividades debe en registrarse y con qué niveles de detalle se determinará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

4.3.9 Registro de la gestión de incidencias [op.exp.9].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se registrarán todas las actuaciones relacionadas con la gestión de incidencias, 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 las incidencias, 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.
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 incidencias 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	no aplica	aplica

Categoría ALTA

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
	no aplica	no aplica	aplica

Categoría ALTA

Se establecerá un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

a) Grado de implantación de las medidas de seguridad.
b) Eficacia y eficiencia de las medidas de seguridad.
c) Impacto de los incidentes de seguridad.

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 incidencias 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 abandonen 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 incidencias, de pérdidas o sustracciones.

c) Se establecerá un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el equipo se conecte a redes, en particular si el equipo se conecta a redes públicas.

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, preferentemente, productos certificados [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 alguna (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.º La alteración de la información en transito

2.º La inyección de información espuria

3.º El secuestro de la sesión por una tercera parte

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 valorará positivamente en empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.
b) Se emplearán, preferentemente, productos certificados [op.pl.5].

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, preferentemente, productos certificados [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	C		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

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.

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.
b) Se destruirán de forma segura los soportes, en los siguientes casos:

1.º Cuando la naturaleza del soporte no permita un borrado seguro.
2.º Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	todas		
categoría	básica	media	alta
	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.

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	+	++

La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.
La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido.
Cuando se emplee firma electrónica:

a) El signatario será la parte que se hace responsable de la información, en la medida de sus atribuciones.
b) Se dispondrá de una Política de Firma Electrónica, aprobada por el órgano superior competente que corresponda.

Nivel BAJO

Se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

1. Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
b) Se emplearán, preferentemente, certificados reconocidos.
c) Se emplearán, preferentemente, dispositivos seguros de firma.

2. 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:

a) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

1.º Certificados.
2.º Datos de verificación y validación.

b) Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.

c) 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 a) y b).

d) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes a) y b).

Nivel ALTO

Se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en la nivel Medio, además de las siguientes:

a) Se usarán certificados reconocidos.
b) Se usarán dispositivos seguros de creación de firma.
c) Se emplearán, preferentemente, productos certificados [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].

5.7.6 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
	no aplica	aplica	=

Nivel MEDIO

Se realizarán copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada.

Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de respaldo deberán abarcar:

a) Información de trabajo de la organización.

b) Aplicaciones en explotación, incluyendo los sistemas operativos.

c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

d) 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		
categoría	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».

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. 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.

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 incidencias.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información, serán los siguientes:

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. 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 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 las incidencias que se den. Además de resolverlas 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 99.4 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el artículo 18 del Real Decreto /, de de por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

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.»

§ 4

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: 8 de noviembre de 2011
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. Las Administraciones públicas mantendrán actualizado un Inventario de Información Administrativa, que incluirá los procedimientos administrativos y servicios que prestan de forma clasificada y estructurados en familias, con indicación del nivel de informatización de los mismos. Asimismo mantendrán una relación actualizada de sus órganos administrativos y oficinas de registro y atención al ciudadano, y sus relaciones entre ellos. Dichos órganos y oficinas se codificarán de forma unívoca y esta codificación se difundirá entre las Administraciones públicas.

2. Cada Administración pública regulará la forma de creación y mantenimiento de este Inventario, que se enlazará e interoperará con el Inventario de la Administración General del Estado en las condiciones que se determinen por ambas partes y en el marco de lo previsto en el presente real decreto; en su caso, las Administraciones públicas podrán hacer uso del citado Inventario centralizado 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) Las definiciones de norma y especificación técnica establecidas 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 las normas y reglamentaciones técnicas.

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, aprobado por el Consejo Superior de Administración Electrónica, para su interconexión a través de las redes de comunicaciones de las Administraciones públicas.

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 y de la documentación asociada, y de otros objetos de información de los cuales las Administraciones públicas sean titulares de los derechos de propiedad intelectual y que éstas puedan poner a disposición de otras Administraciones públicas y de los ciudadanos, sin contraprestación y sin necesidad de convenio, tendrán en cuenta que el fin perseguido es el aprovechamiento y la reutilización,

así como la protección contra su apropiación en exclusiva por parte de terceros, en condiciones tales que eximan de responsabilidad al cedente por el posible mal uso por parte del cesionario, así como la no obligación a la asistencia técnica o el mantenimiento por parte del cedente, ni de compensación alguna en caso de errores en la aplicación.

2. Las administraciones utilizarán para las aplicaciones que declaren como de fuentes abiertas aquellas 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. 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.

Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio de aplicaciones para su libre reutilización que podrá ser accedido a través del Centro de Transferencia de Tecnología.

2. Las Administraciones públicas enlazarán los directorios de aplicaciones para su libre reutilización a los que se refiere el artículo 46 de la Ley 11/2007, de 22 de junio, entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones públicas 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.

4. Las Administraciones públicas procurarán la publicación del código de las aplicaciones, en desarrollo o finalizadas, en los directorios de aplicaciones para su libre reutilización con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia.

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 la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

2. Las Administraciones públicas aprobarán y publicarán su política de firma electrónica y de certificados partiendo de la norma técnica establecida a tal efecto en disposición adicional primera, que podrá convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto.

3. Las Administraciones públicas receptoras de documentos electrónicos firmados permitirán la validación de las firmas electrónicas contra la política de firma indicada en la firma del documento electrónico, siempre que dicha política de firma se encuentre dentro de las admitidas por cada Administración pública para el reconocimiento mutuo o multilateral con otras Administraciones públicas.

4. 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.

Dichos certificados serán los definidos en la Ley 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos.

5. La política de firma electrónica y de certificados, mencionada en el apartado primero del presente artículo, establecerá las características técnicas y operativas de la lista de prestadores de servicios de certificación de confianza que recogerá los certificados reconocidos e interoperables entre las Administraciones públicas y que se consideren fiables para cada nivel de aseguramiento concreto, tanto en el ámbito nacional como europeo. La lista que establezca la Administración General del Estado podrá ser utilizada como referencia por otras Administraciones públicas para definir sus listas de servicios de confianza para aplicación dentro de sus ámbitos competenciales.

6. Las aplicaciones usuarias de certificados electrónicos y firma electrónica:

a) Se atendrán a la política de firma electrónica y de certificados aplicable en su ámbito en relación con los diversos aspectos contemplados y particularmente con 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.

b) Permitirán los mecanismos de acreditación y representación de los ciudadanos en materia de identificación y firma electrónica, previstos en la normativa correspondiente.

Artículo 19. *Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación.*

1. De acuerdo con lo previsto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, sobre obligaciones de los prestadores de servicios de certificación, en relación con la interoperabilidad, dichos prestadores cumplirán con lo indicado en los apartados siguientes.

2. En relación con la interoperabilidad organizativa, los prestadores de los servicios de certificación dispondrán de lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) Establecimiento de los usos de los certificados expedidos de acuerdo con un perfil dado y sus posibles límites de uso.

b) Prácticas al generar los certificados que permitan posteriormente la aplicación de unos mecanismos de descubrimiento y extracción inequívoca de los datos de identidad del certificado.

c) Definición de la información de los certificados o relacionada con ellos que será publicada por parte del prestador, debidamente catalogada.

d) Definición de los posibles estados en los que un certificado pueda encontrarse a lo largo de su ciclo de vida.

e) Los niveles de acuerdo de servicio definidos y caracterizados para los servicios de validación y de sellado de fecha y hora.

3. En relación con la interoperabilidad semántica, los prestadores de servicios de certificación aplicarán lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) La definición de los perfiles de certificados que describirán, mediante mínimos, el contenido obligatorio y opcional de los diferentes tipos de certificados que emiten, así como la información acerca de la sintaxis y semántica de dichos contenidos.

b) Establecimiento de los campos cuya unicidad de información permitirá su uso en labores de identificación.

4. En relación con la interoperabilidad técnica, los prestadores de los servicios de certificación aplicarán lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) Los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos, estado de los certificados, dispositivos seguros de creación de firma, programas controladores, dispositivos criptográficos, interfaces de programación, tarjetas criptográficas, conservación de documentación relativa a los certificados y servicios, límites de los certificados, conforme a lo establecido en el artículo 11.

b) La incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación por parte de los prestadores.

c) Los mecanismos de publicación y de depósito de certificados y documentación asociada admitidos entre Administraciones públicas.

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) 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) 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) 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) Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) 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) 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) 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) 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 las Entidades de Derecho Público vinculadas o dependientes de aquéllas.

i) Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas.

j) Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) 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) 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.

2. El Ministerio de la Presidencia, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, aprobará las normas

técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado para la Función Pública. Para la redacción y mantenimiento de las normas técnicas de interoperabilidad indicadas en el apartado 1 se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

3. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Inventario de procedimientos administrativos y servicios prestados: contendrá información de los procedimientos y servicios, clasificada con indicación del nivel de informatización de los mismos, 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: publicará los modelos de datos de intercambio tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, junto con las definiciones y codificaciones asociadas; proporcionará funciones de repositorio, generación de formatos para procesamiento automatizado, colaboración, publicación y difusión de los modelos de datos que faciliten la interoperabilidad semántica entre las Administraciones públicas y de éstas con los ciudadanos; se enlazará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Directorio de aplicaciones para su libre reutilización: 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.

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.*

CENATIC, Fundación Pública Estatal, constituida por el Ministerio de Industria, Turismo y Comercio, a través de Red.es, podrá impulsar proyectos de software de fuentes abiertas dirigidos a la mejor implantación de las medidas de interoperabilidad contempladas en el presente real decreto y, al objeto de fomentar la reutilización y facilitar la interoperabilidad, se encargará de la puesta en valor y difusión de todas aquellas aplicaciones que sean declaradas de fuentes abiertas por las Administraciones Públicas.

Disposición adicional cuarta. *Instituto Nacional de Tecnologías de la Comunicación.*

INTECO, como centro de excelencia promovido por el Ministerio de Industria, Turismo y Comercio para el desarrollo de la sociedad del conocimiento, podrá desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de interoperabilidad contempladas en el presente real decreto.

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.

Familia: Se entiende por tal la agrupación de procedimientos administrativos atendiendo a criterios genéricos de similitud por razón de esquema de tramitación, documentación de entrada y salida e información, dejando al margen criterios de semejanza en la materia objeto del procedimiento, órgano competente, u otra información análoga.

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.

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, la plataforma de verificación de certificados electrónicos.

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.

§ 5

Orden HAP/566/2013, de 8 de abril, por la que se regula el Registro Electrónico Común

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 88, de 12 de abril de 2013
Última modificación: 1 de enero de 2014
Referencia: BOE-A-2013-3862

El artículo 24 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, establece que las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones y señala que los registros podrán admitir documentos normalizados que se cumplimenten de acuerdo con formatos preestablecidos, o bien cualquier solicitud escrito o comunicación distinta de los anteriores. Dicho precepto establece que, en cada Administración Pública existirá, al menos, un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidas a dicha Administración Pública. Asimismo, para un mejor servicio a los ciudadanos prevé que las Administraciones Públicas, mediante Convenios de colaboración, puedan habilitar a sus registros para la recepción de solicitudes, escritos y comunicaciones de la competencia de otra Administración.

Para dar cumplimiento a estas previsiones legales, el artículo 31 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada Ley 11/2007, de 22 de junio, establece la creación, naturaleza y funcionamiento del Registro Electrónico Común con el fin de permitir la presentación electrónica de escritos, solicitudes y comunicaciones dirigidas a la Administración General del Estado y a sus Organismos públicos. Conforme a lo previsto en el citado artículo 31, los requisitos y condiciones de funcionamiento del Registro Electrónico Común se establecerán mediante orden del Ministro de la Presidencia. De esta forma la Orden PRE/3523/2009, de 29 de diciembre, procedió a dar cumplimiento al referido mandato, determinando la regulación del referido Registro Electrónico Común.

Por su parte, la Orden TAP/1955/2011, de 5 de julio, por la que se crea y regula el registro electrónico del Ministerio de Política Territorial y Administración Pública y por la que se modifica la Orden PRE/3523/2009, de 29 de diciembre, por la que se regula el Registro Electrónico Común, abre la posibilidad de que éste actúe como registro específico de los procedimientos de inscripción y pago de tasas de los procesos selectivos que impliquen a varios Departamentos u Organismos.

No obstante, la nueva estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas establecida por el Real Decreto 256/2012, de 27 de enero, hace preciso adecuar la regulación en materia de Registro Electrónico Común a los cambios organizativos producidos. Asimismo, la actualización de la regulación del Registro Electrónico Común responde a lo establecido en los Esquemas Nacionales de Seguridad y de Interoperabilidad en el ámbito de la Administración Electrónica, aprobados por los Reales

Decretos 3/2010 y 4/2010, de 8 de enero, y en particular, en la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de Asientos entre las Entidades Registrales, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, que sienta las bases para la interconexión de registros entre las Administraciones Públicas y su interconexión con el Registro Electrónico Común, objeto de la disposición adicional segunda de esta nueva regulación.

De acuerdo con lo señalado anteriormente, se considera necesario, a efectos de una mayor seguridad jurídica, refundir en una sola orden la regulación existente sobre el Registro Electrónico Común.

Para la creación de un fichero, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en su artículo 20, así como el artículo 52 del Reglamento de desarrollado de dicha ley, aprobado por Real Decreto 1720/2007, de 21 de diciembre, establece que solo podrá hacerse por disposición de carácter general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

La presente orden ha sido sometida al previo informe de la Agencia Española de Protección de Datos de conformidad con lo dispuesto en el artículo 37, párrafo h), de la Ley Orgánica 15/1999, de 13 de diciembre.

En uso de la atribución que me ha sido conferida en el artículo 31.5 del Real Decreto 1671/2009, de 6 de noviembre, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. La presente orden tiene por objeto la regulación de los requisitos y condiciones de funcionamiento del Registro Electrónico Común, creado por el artículo 31 del 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.

2. De conformidad con lo previsto en el artículo 31.3 del citado Real Decreto, el Registro Electrónico Común posibilitará la presentación de cualesquiera solicitudes, escritos y comunicaciones dirigidas a la Administración General del Estado y a sus Organismos públicos, y está habilitado para la recepción y remisión de solicitudes, escritos y comunicaciones, presentados al amparo del artículo 24.2.b) de la Ley 11/2007, de 22 de junio.

En todo caso, de acuerdo con lo establecido en el artículo 31.4 de dicho real decreto, el Registro Electrónico Común informará al ciudadano y le redirigirá, cuando proceda, a los registros competentes para la recepción de aquellos documentos que dispongan de aplicaciones específicas para su tratamiento.

3. El ámbito del Registro Electrónico Común es la Administración General del Estado y los Organismos Públicos adscritos o dependientes de la misma.

Artículo 2. *Órganos competentes.*

1. El Registro Electrónico Común será gestionado por la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas, a través de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. Corresponde a la Secretaria de Estado de Administraciones Públicas, la modificación del formulario electrónico de propósito general para la presentación en el Registro Electrónico Común de los escritos a los que se refiere el artículo 24.2.b) de la Ley 11/2007, de 22 de junio, que se incluye en el anexo I de la presente orden, así como la aprobación de otros formularios que, en su caso, resulten precisos para la presentación de los escritos en dicho Registro.

2. De acuerdo con lo previsto en los artículos 9 y 31.4 del Real Decreto 1671/2009, de 6 de noviembre, los Departamentos ministeriales y Organismos públicos participarán en la gestión del Registro Electrónico Común, y serán responsables de mantener actualizada la información que éste proporcione sobre servicios, procedimientos y trámites que cuentan con aplicaciones específicas y formularios normalizados en los Registros de su competencia.

Asimismo, serán responsables del acceso al Registro Electrónico Común y el traslado, en su caso, al registro competente para su tramitación de los escritos recibidos en el Registro Electrónico Común que tengan como destinatario al Ministerio u Organismo de que se trate.

Artículo 3. *Inscripción en procesos selectivos.*

El Registro Electrónico Común actuará como registro específico para la inscripción y pago de la correspondiente tasa en las convocatorias de procesos selectivos en relación con el ingreso en Cuerpos o Escalas de personal funcionario o en plazas de personal laboral adscritos a la Administración General del Estado y sus Organismos públicos vinculados o dependientes, así como para la aportación de documentación adicional, cuyos formularios de inscripción figuren en la dirección electrónica de acceso al registro, para las que exista un Acuerdo de encomienda de gestión entre el órgano convocante y el Ministerio de Hacienda y Administraciones Públicas por el cual se encomiende a este último la gestión de la inscripción y pago por vía telemática.

El formulario específico a utilizar para la presentación de solicitudes respecto a la inscripción en procesos selectivos, se recoge en el anexo II de la presente orden y estará disponible en su sede electrónica.

Artículo 4. *Registro Electrónico de Apoderamientos.*

El Registro Electrónico Común actuará como registro específico para la inscripción en el Registro Electrónico de Apoderamientos, así como para la aportación de documentación adicional en dicho registro, cuyos formularios de inscripción fueron publicados en la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos.

Artículo 5. *Acceso al Registro Electrónico Común.*

1. El acceso al Registro Electrónico Común estará disponible en la sede electrónica del Punto de Acceso General de la Administración General del Estado, regulado por el artículo 9 del Real Decreto 1671/2009, de 6 de noviembre.

2. La sede electrónica del Punto de Acceso General contendrá la información que facilite a los interesados la utilización de los procedimientos de identificación y firma electrónica admitidos, o el enlace con la dirección en que dicha información se contenga. Asimismo, incluirá información detallada sobre la utilización, validación y conservación de los ficheros de acuse de recibo, entregados como consecuencia de la presentación de cualquier tipo de documento ante el Registro Electrónico Común.

3. La sede electrónica incluirá una relación de los documentos electrónicos normalizados correspondientes a los Departamentos ministeriales y Organismos públicos, y un enlace con la sede electrónica a través de la cual debe realizarse la presentación de dichos escritos ante el registro competente.

4. En la sede electrónica del Punto de Acceso General estará disponible para su consulta la orden por la que se regula el Registro Electrónico Común.

Artículo 6. *Documentos admisibles.*

1. El Registro Electrónico Común admitirá cualquier solicitud, escrito o comunicación, dirigida a la Administración General del Estado o a sus Organismos públicos que, conforme a lo previsto en el artículo 24.2.b) de la Ley 11/2007, de 22 de junio, no se corresponda con un documento electrónico normalizado que pueda cumplimentarse de acuerdo con formatos preestablecidos en su formulario correspondiente.

El formulario de propósito general a utilizar para la presentación de solicitudes, escritos y comunicaciones en el Registro Electrónico Común se recoge en el anexo I de la presente orden y estará disponible en su sede electrónica.

2. El Registro Electrónico Común admitirá asimismo documentación complementaria al escrito de iniciación mediante documentos electrónicos, incluyendo copias digitalizadas, conforme a los requisitos, condiciones y exigencias del artículo 35.2 de la Ley 11/2007, de 22 de junio. De acuerdo con los instrumentos informáticos y vías de comunicación disponibles, podrá limitarse la extensión máxima de los documentos complementarios a presentar en una sola sesión.

La aportación de la documentación complementaria que se realice en el Registro Electrónico Común en un momento posterior, ya sea por las razones técnicas aludidas en el

párrafo anterior o de otra índole, se llevará a cabo mediante una nueva presentación que incluirá, al menos, la referencia al número o código de registro individualizado al que se refiere el artículo 8.1 de esta orden, del escrito de iniciación, o la información que permita identificarlo.

3. Cuando requiriéndose la presentación de una solicitud, escrito o comunicación mediante la utilización de documentos normalizados en el registro competente al efecto, conforme a lo previsto en el artículo 32 del Real Decreto 1671/2009, de 6 de noviembre, esta presentación se realice en el Registro Electrónico Común, la misma se admitirá y registrará, si bien el órgano destinatario podrá requerir al ciudadano la subsanación de acuerdo con lo previsto en el artículo 29.3 del citado Real Decreto.

Los documentos admitidos en el Registro Electrónico Común se ajustarán a lo establecido en 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, así como a lo establecido en la Resolución de la Secretaría de Estado de Administraciones Públicas, de 3 de octubre de 2012, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares.

4. La presentación de solicitudes, escritos o comunicaciones dirigidos a órganos o entidades dependientes de otras Administraciones Públicas se tendrá por no realizada. En tal caso, se comunicará al interesado tal circunstancia, a través del medio elegido por éste en el momento de la presentación del escrito y se le informará sobre el sitio electrónico donde puede encontrar la referencia de los registros y lugares habilitados para la presentación conforme a las normas en vigor.

Todo ello se entiende sin perjuicio de lo previsto en la disposición adicional primera de la presente orden, que prevé que el Registro Electrónico Común, a través de los correspondientes Convenios, pueda ser habilitado para la remisión, recepción e intercambio de solicitudes, escritos y comunicaciones de la competencia de otras Administraciones Públicas.

Artículo 7. *Acreditación de la identidad.*

1. Los documentos electrónicos podrán ser presentados ante el Registro Electrónico Común por los interesados, o por sus representantes cuando estén operativos los sistemas informáticos para la comprobación y validación de la representación a través de:

a) El régimen de representación habilitada regulado por el artículo 23 de la Ley 11/2007, de 22 de junio, y los artículos 13 y 14 del Real Decreto 1671/2009, de 6 de noviembre.

b) Su acreditación ante el Registro electrónico de apoderamientos, en los términos previstos en la Orden HAP/1637/2012, de 5 de julio, por la que se regula aquel.

2. El firmante del documento podrá acreditar su identidad ante el Registro Electrónico Común mediante los sistemas de firma electrónica incorporados al documento nacional de identidad o mediante sistemas de firma electrónica avanzada a los que se refiere el artículo 13.2 de la Ley 11/2007, de 22 de junio, o a través de funcionarios públicos habilitados, mediante el procedimiento previsto en el artículo 22 de dicha Ley.

3. El Registro Electrónico Común permitirá la utilización de todos los certificados respecto a los que se acuerde la admisión general en el ámbito de la Administración General del Estado.

Artículo 8. *Acuse de recibo.*

1. El Registro Electrónico Común emitirá automáticamente por el mismo medio un recibo electrónico firmado mediante alguno de los sistemas de firma previstos en el artículo 18 de la Ley 11/2007, de 22 de junio, con el siguiente contenido:

a) El número o código de registro individualizado.

b) La fecha y hora de presentación.

c) La copia autenticada del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.

d) En su caso, la enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.

e) En el caso de la inscripción en los procesos selectivos a que se refiere el artículo 3, información del plazo máximo establecido normativamente para la resolución y notificación del procedimiento, así como de los efectos que pueda producir el silencio administrativo, cuando sea automáticamente determinable.

2. El acuse de recibo indicará que el mismo no prejuzga la admisión definitiva del escrito cuando concurra alguna de las causas de rechazo contenidas en el artículo 29.1 del Real Decreto 1671/2009, de 6 de noviembre.

Artículo 9. *Presentación de documentos. Fecha y hora oficial. Cómputo de plazos.*

1. El Registro Electrónico Común permitirá la presentación de solicitudes, escritos y comunicaciones todos los días del año, durante las veinticuatro horas del día, sin perjuicio de las interrupciones de mantenimiento técnico u operativo contempladas en el artículo 30.2 del Real Decreto 1671/2009, de 6 de noviembre, que se anunciarán con la antelación que resulte posible en la sede electrónica del Registro Electrónico Común.

Cuando por tratarse de interrupciones no planificadas que impidan la presentación de escritos no resulte posible realizar su anuncio con antelación, se actuará conforme a lo establecido en el artículo 30.2 del Real Decreto 1671/2009, de 6 de noviembre, a cuyo efecto, siempre que una norma legal no lo impida expresamente, se dispondrá por el tiempo imprescindible la prórroga de los plazos de inminente vencimiento, de lo que se dejará constancia en la sede electrónica.

2. Conforme a lo establecido en el artículo 26.1 de la Ley 11/2007, de 22 de junio, la fecha y hora a computar en las anotaciones del Registro Electrónico Común será la oficial de la sede electrónica de acceso, debiendo adoptarse las medidas precisas para asegurar su integridad.

3. El calendario de días inhábiles a efectos del Registro Electrónico Común será el que se determine en la Resolución publicada cada año en el «Boletín Oficial del Estado» para todo el territorio nacional por el Ministerio de Hacienda y Administraciones Públicas, en cumplimiento del artículo 48.7 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

4. El cómputo de plazos se realizará conforme a lo dispuesto en los apartados 3, 4 y 5 del artículo 26 de la Ley 11/2007, de 22 de junio. El inicio del cómputo de plazos vendrá determinado por la fecha y hora de entrada en el Registro del destinatario. La fecha de presentación, y sus consecuencias a efectos de cómputo de plazos, se comunicarán expresamente al ciudadano en el justificante de registro, que se generará automáticamente tras cada presentación, y podrá descargarse adicionalmente mediante una consulta al registro realizado.

Artículo 10. *Fichero de Protección de Datos.*

(Derogado)

Artículo 11. *Responsabilidad.*

Los usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su autenticación en el acceso a los servicios prestados mediante administración electrónica, el establecimiento de la conexión precisa y la utilización de la firma electrónica, así como de las consecuencias que pudieran derivarse del uso indebido, incorrecto o negligente de los mismos. Igualmente será responsabilidad del usuario la adecuada custodia y manejo de los ficheros que le sean devueltos por el Registro Electrónico Común como acuse de recibo.

Los departamentos ministeriales y organismos públicos destinatarios de los escritos presentados en el Registro Electrónico Común serán responsables de la custodia y manejo de los correspondientes ficheros.

Disposición adicional primera. *Escritos dirigidos a otras Administraciones Públicas.*

De acuerdo con lo previsto en el artículo 24.3 de la Ley 11/2007, de 22 de junio, el Registro Electrónico Común podrá ser habilitado para la remisión, recepción e intercambio de solicitudes, escritos y comunicaciones de la competencia de otras Administraciones Públicas, en la forma que se determine en los correspondientes Convenios.

Disposición adicional segunda. *Interoperabilidad de los registros públicos.*

La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado de Administraciones Públicas, certificará las herramientas y mecanismos que se pongan en funcionamiento para garantizar el acceso y la interoperabilidad con el Registro Electrónico Común, así como para garantizar la interconexión de los registros, por parte del resto de las Administraciones Públicas, de conformidad con lo señalado en 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.

Disposición adicional tercera. *No incremento de gasto público.*

Las medidas contenidas en esta orden se atenderán con los medios personales y materiales existentes en el Ministerio de Hacienda y Administraciones Públicas, y en ningún caso podrá generar incremento de gasto público.

Disposición transitoria única. *Acceso al Registro Electrónico Común.*

En tanto no se produzca la entrada en funcionamiento de la sede electrónica del Punto de Acceso General de la Administración General del Estado, el acceso al Registro Electrónico Común estará disponible en la sede electrónica del portal nacional de ciudadanos y empresas (sede.060.gob.es.), y en el propio portal (www.060.es).

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas la Orden PRE/3523/2009, de 29 de diciembre, por la que se regula el Registro Electrónico Común, y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta orden.

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».

Madrid, 8 de abril de 2013.–El Ministro de Hacienda y Administraciones Públicas, Cristóbal Montoro Romero.

ANEXO I

Formulario de propósito general

1. Datos del formulario:

Tipo de documento (obligatorio).
Número de identificación (obligatorio).
Nombre (obligatorio).
Primer apellido (obligatorio).
Segundo apellido (obligatorio).
País (obligatorio).
Provincia (obligatorio).
Localidad (obligatorio).
Tipo de vía (obligatorio).
Nombre y número de vía (obligatorio).
Bloque.

Escalera.
Piso.
Puerta.
Código postal (obligatorio).
Teléfono de contacto.
Correo electrónico.
Teléfono móvil.

2. Datos de la solicitud:

Organismo destinatario (obligatorio).
Asunto: (obligatorio).
Expone: (obligatorio).
Solicita: (obligatorio).

3. Documentos anexos:

Documentos (hasta cinco).

4. Alertas:

Alerta SMS.
Alerta mail.

ANEXO II

Formulario de inscripción a pruebas selectivas

1. Datos del formulario:

N.º justificante (obligatorio).
Nombre (obligatorio).
Primer apellido (obligatorio).
Segundo apellido (obligatorio).
Correo electrónico (obligatorio).
NIF (obligatorio).
Nacionalidad.
Fecha de nacimiento (obligatorio).
Sexo (obligatorio).
Domicilio-calle o plaza (obligatorio).
Domicilio-municipio (obligatorio).
Domicilio-provincia (obligatorio).
Domicilio-código postal (obligatorio).
Domicilio-país (obligatorio).
Domicilio-teléfonos (obligatorio).
Convocatoria-Cuerpo y Escala (obligatorio).
Convocatoria-Especialidad.
Convocatoria-Centro gestor (obligatorio).
Convocatoria-importe (obligatorio).
Convocatoria-Ministerio (obligatorio).
Convocatoria-fecha BOE (obligatorio).
Convocatoria-forma acceso (obligatorio).
Convocatoria-ejercicio (obligatorio).
Convocatoria-provincia de examen (obligatorio).
Porcentaje discapacidad.
Reserva plaza.
Adaptación que se solicita.
Títulos académicos-exigidos en la convocatoria (obligatorio).
Títulos académicos-otros títulos.
Datos a consignar según las bases de la convocatoria-datos A.
Datos a consignar según las bases de la convocatoria-datos B.

Datos a consignar según las bases de la convocatoria-datos C.
Dirigido a (obligatorio).
Consiente verificación de datos (obligatorio).

2. Autoliquidación del pago de la tasa:

Importe (obligatorio).
Tipo de pago: (obligatorio).
Causa de exención o reducción.
Fecha de pago: (obligatorio).
NRC.
Entidad.

3. Documentos anexos.

ANEXO III

Fichero de datos personales

(Derogado)

§ 6

Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 177, de 25 de julio de 2012
Última modificación: 1 de enero de 2014
Referencia: BOE-A-2012-9931

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, crea, en su artículo 15, el registro electrónico de apoderamientos para actuar ante la Administración General del Estado y sus organismos públicos dependientes o vinculados. La creación de este registro tiene como finalidad mejorar la atención a los ciudadanos, poniendo a su disposición un instrumento que facilite la acreditación, ante los órganos de la Administración, de los apoderamientos concedidos para la realización de trámites administrativos, por lo que la creación del registro no supone ninguna modificación de la regulación de la representación existente en nuestro ordenamiento y se realiza sin perjuicio de la existencia, actual o futura, de otros registros similares de ámbito más limitado en la Administración General del Estado. En la medida en que su finalidad es la mejora del servicio público, el acceso al registro tiene carácter absolutamente voluntario para los ciudadanos, que además van a poder determinar los trámites y actuaciones a los que, entre los que se encuentren en cada momento habilitados en el registro, se extienden los apoderamientos concedidos.

La incorporación de las tecnologías de la información a la actividad administrativa posibilita la realización de trámites o actuaciones por medios electrónicos, lo que supone una clara mejora del servicio prestado a los ciudadanos, en la medida en que éstos obtienen una respuesta administrativa inmediata que permite atender mejor sus necesidades. En otros casos, esa automatización facilita tanto el mejor ejercicio de sus derechos como el puntual cumplimiento de sus obligaciones.

Por otro lado, el artículo 32 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, regula la representación de los ciudadanos ante las Administraciones Públicas. Del mismo modo, el artículo 23 de la Ley 11/2007, de 22 de junio, establece que las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados.

En este contexto jurídico, y con el único objetivo de facilitar al ciudadano que así lo desee el acceso electrónico a los Servicios Públicos, se creó el Registro electrónico de apoderamientos. De esta manera se habilita una nueva vía al ciudadano para apoderar, a cualquier otro ciudadano o empresa, para que actúe en su nombre. De acuerdo con el anexo de la Ley 11/2007, de 22 de junio, se considera ciudadano a cualesquiera persona física,

persona jurídica y ente sin personalidad que se relacione, o sea susceptible de relacionarse, con las Administraciones Públicas.

Conforme a lo previsto en el apartado 5 del citado artículo 15 del Real Decreto 1671/2009, de 6 de noviembre, los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos se establecerán mediante Orden del Ministro de la Presidencia. En la actualidad y de acuerdo con lo dispuesto en el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, el ministerio competente para dictar la presente Orden es el Ministerio de Hacienda y Administraciones Públicas. La presente Orden recoge todos los aspectos enunciados en el Real Decreto 1671/2009, de 6 de noviembre.

Esta norma ha sido sometida al previo informe de la Agencia Española de Protección de Datos. Asimismo, esta norma ha recibido el informe favorable del Consejo Superior de Administración Electrónica.

En uso de la atribución que me ha sido conferida en el artículo 15.5 del Real Decreto 1671/2009, de 6 de noviembre, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. La presente Orden tiene por objeto la regulación de los requisitos y condiciones de funcionamiento del Registro electrónico de apoderamientos, creado por el artículo 15 del Real Decreto 1671/2009, de 6 de noviembre.

2. En el Registro electrónico de apoderamientos se podrán hacer constar las representaciones que los ciudadanos otorguen a terceros para actuar en su nombre de forma electrónica ante la Administración General del Estado y sus organismos públicos vinculados o dependientes.

3. Sólo se inscribirán en el Registro las representaciones que los interesados otorguen voluntariamente, de conformidad con el artículo 32 de la Ley 30/1992, de 26 de noviembre. Queda así excluida la inscripción de las representaciones legales.

4. El ámbito del Registro Electrónico de Apoderamientos se extiende a la Administración General del Estado y a los organismos públicos vinculados o dependientes de la misma. Sólo podrán comprobar la representación o apoderamiento mediante el acceso al Registro electrónico de apoderamientos aquellos ministerios u organismos públicos que se suscriban al Registro.

5. La representación que se inscriba en el Registro sólo será válida para los trámites y actuaciones por medios electrónicos de su competencia que, con carácter previo y en los términos especificados en el artículo 9, haya determinado cada departamento ministerial u organismo público suscrito a aquel, lo que oportunamente será comunicado al Registro.

6. El Registro Electrónico de Apoderamientos, regulado en esta Orden, no participa de la naturaleza jurídica de los registros electrónicos regulados en el artículo 24 de la Ley 11/2007, de 22 de junio.

Artículo 2. *Órganos competentes.*

1. El Registro electrónico de apoderamientos será gestionado por el Ministerio de Hacienda y Administraciones Públicas, a través de la Secretaría de Estado de Administraciones Públicas, quedando a cargo del mismo la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.

2. Los ministerios y organismos públicos vinculados o dependientes serán los competentes para dar de alta, modificar y dar de baja en el Registro los trámites y actuaciones por medios electrónicos de su competencia para los que será válida la representación incorporada a dicho Registro.

3. La inscripción en el Registro será automática para los apoderamientos que se otorguen de persona física a persona física y se tramiten electrónicamente. Cuando el poderdante sea una persona física y el apoderamiento se produzca por comparecencia ante un funcionario expresamente autorizado para dar de alta en el Registro los apoderamientos, será aquél el responsable de la inscripción. En cualquier otro supuesto, el órgano competente para dicha inscripción y para, en su caso, requerir al interesado eventuales subsanaciones de defectos en la representación, será el que ostente la competencia sobre

los trámites o actuaciones por medios electrónicos objeto del apoderamiento. En este último caso, el apoderamiento deberá estar referido a trámites de un único órgano.

Artículo 3. *Incorporación de los apoderamientos al Registro.*

1. En la tramitación electrónica de las solicitudes de inscripción de apoderamientos en el Registro se estará a lo dispuesto en el capítulo II del título tercero de la Ley 11/2007, de 22 de junio.

2. Cuando el poderdante es una persona física, la inscripción de apoderamientos en el Registro podrá llevarse a efecto mediante uno de estos procedimientos:

a) Por Internet, mediante el uso de los sistemas de identificación y autenticación previstos en el artículo 13.2.a) y b) de la Ley 11/2007, de 22 de junio. La inscripción del apoderamiento se realizará mediante el formulario que figura en el anexo I de esta Orden, a excepción de los datos asociados a documento público o privado con firma notarialmente legitimada. La solicitud quedará anotada en el Registro Electrónico Común. Los efectos de la inscripción en el Registro electrónico de apoderamientos serán, en este caso, inmediatos.

b) Mediante comparecencia personal del poderdante en las oficinas de atención al ciudadano 060, dependientes del Ministerio de Hacienda y Administraciones Públicas, en las oficinas consulares o en las oficinas dependientes de los organismos adheridos al Registro que estos determinen, mediante el empleo del formulario del Anexo I. En el formulario deberá constar la firma del poderdante y la identificación y firma del funcionario ante quien se comparece que, en todo caso, deberá estar expresamente autorizado para dar de alta en el Registro los apoderamientos. La solicitud quedará anotada en el Registro Electrónico Común. Será inscrita en el Registro electrónico de apoderamientos por el funcionario y surtirá efectos a partir de esta inscripción, que en todo caso no deberá ser posterior en dos días hábiles a la inscripción en el Registro Electrónico Común.

c) Poder otorgado mediante documento público o documento privado con firma notarialmente legitimada, presentado en una oficina adherida al Registro. La solicitud quedará anotada en el Registro Electrónico Común. En este caso, el órgano u organismo competente de los trámites objeto del apoderamiento solicitará, en su caso, a su Asesoría Jurídica un informe sobre el poder presentado por el representante de la entidad, que deberá ser emitido en un plazo no superior a siete días. La posterior inscripción del apoderamiento en el Registro, que deberá hacerse en un plazo no superior a dos días hábiles desde la emisión del informe de Asesoría Jurídica, o la eventual solicitud de subsanación de errores al interesado, será llevada a cabo por el órgano u organismo competente. El poder será incorporado al Registro, como un documento electrónico, según la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico. En este caso, el documento de acreditación del apoderamiento deberá ajustarse al contenido recogido en el formulario del Anexo I.

3. Cuando el poderdante es una persona jurídica o ente sin personalidad, la inscripción de apoderamientos en el Registro podrá llevarse a efecto mediante uno de estos procedimientos:

a) Por comparecencia personal del representante legal de la entidad, en las oficinas de atención al ciudadano 060, dependientes del Ministerio de Hacienda y Administraciones Públicas, en las oficinas consulares o en las oficinas dependientes de los organismos adheridos al Registro que éstos determinen, mediante el empleo del formulario del Anexo I. La solicitud quedará anotada en el Registro Electrónico Común. El organismo competente de los trámites objeto del apoderamiento solicitará, en su caso, a su Asesoría Jurídica un informe sobre los poderes presentados por el representante de la entidad, que deberá ser emitido en un plazo no superior a siete días. La posterior inscripción del apoderamiento en el Registro, que deberá hacerse en un plazo no superior a dos días hábiles desde la emisión del informe de Asesoría Jurídica, o la eventual solicitud de subsanación de errores al interesado, será llevada a cabo por el órgano u organismo competente. Los poderes presentados por el representante de la entidad serán incorporados al Registro, como un documento electrónico, según la Norma Técnica de Interoperabilidad de Documento

Electrónico, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública.

b) Por Internet, mediante el uso por el representante de la entidad de los sistemas de identificación y autenticación previstos en el artículo 13.2.a) y b) de la Ley 11/2007, de 22 de junio. Con carácter previo el representante habrá presentado en una oficina adherida al Registro sus poderes como representante. El organismo competente de los trámites objeto del apoderamiento solicitará, en su caso, a su Asesoría Jurídica un informe sobre los poderes presentados por el representante de la entidad, que deberá ser emitido en un plazo no superior a siete días. La posterior inscripción del apoderamiento en el Registro, que deberá hacerse en un plazo no superior a dos días hábiles desde la emisión del informe de Asesoría Jurídica, o la eventual solicitud de subsanación de errores al interesado, será llevada a cabo por el organismo competente.

c) Poder otorgado mediante documento público o documento privado con firma notarialmente legitimada presentado en una oficina adherida al Registro. La solicitud quedará anotada en el Registro Electrónico Común. El órgano u organismo competente de los trámites objeto del apoderamiento solicitará, en su caso, a su Asesoría Jurídica un informe sobre el poder presentado, que deberá ser emitido en un plazo no superior a siete días. La posterior inscripción del apoderamiento en el Registro, que deberá hacerse en un plazo no superior a dos días hábiles desde la emisión del informe de Asesoría Jurídica, o la eventual solicitud de subsanación de errores al interesado, será llevada a cabo por el órgano u organismo competente. El poder presentado será incorporado al Registro, como un documento electrónico, según la Norma Técnica de Interoperabilidad de Documento Electrónico, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública. En este caso, el documento de acreditación del apoderamiento deberá ajustarse al contenido recogido en el formulario del Anexo I.

Artículo 4. *Inscripción de apoderamientos con confirmación explícita del apoderado.*

En el caso de inscripción de apoderamientos para los trámites y actuaciones por medios electrónicos para los que el órgano u organismo competente exija la confirmación del apoderado, será necesaria la aceptación explícita del mismo, que se acreditará por cualquiera de los procedimientos previstos en el artículo anterior. El poder se entenderá como no conferido en tanto no conste en el Registro la mencionada aceptación. La confirmación explícita del apoderado es inexcusable en los supuestos en los que éste deba recibir comunicaciones o notificaciones por vía electrónica, sea cual sea la naturaleza del procedimiento.

Artículo 5. *Comprobación del contenido del apoderamiento.*

1. Cuando el poderdante es una persona física:

a) En los apoderamientos otorgados mediante comparecencia personal del poderdante, en los términos referidos en el artículo 3, punto 2, apartado b), el funcionario que proceda a inscribir un apoderamiento en el Registro electrónico de apoderamientos deberá comprobar el contenido del mismo. A tal efecto, verificará la identidad del compareciente y el contenido del formulario del anexo I.

b) En los apoderamientos otorgados por Internet, la aplicación informática que soporte el Registro únicamente permitirá el alta en el mismo de aquellos apoderamientos que contengan todos los datos solicitados en el formulario del Anexo I. En aquellos casos en los que se detecten anomalías de tipo técnico en la transmisión electrónica del formulario de otorgamiento del poder, dicha circunstancia se pondrá en conocimiento del interesado por el propio sistema, mediante los correspondientes mensajes de error, para que pueda proceder a su inmediata subsanación.

c) En los apoderamientos otorgados mediante documento público o documento privado con firma notarialmente legitimada, el órgano u organismo competente de los trámites objeto del apoderamiento, solicitará, en su caso, informe a su Asesoría Jurídica sobre la suficiencia de los poderes aportados. La inscripción del apoderamiento en el Registro o la eventual solicitud de subsanación de defectos en la representación al interesado, será llevada a cabo por el órgano u organismo competente. Si la subsanación no es atendida en un plazo

máximo de diez días, se comunicará al interesado la imposibilidad de continuar el procedimiento, y la posibilidad de interponer el recurso previsto en artículo 29.2 del Reglamento del Servicio Jurídico del Estado, aprobado por el Real Decreto 997/2003, de 25 de julio.

2. Cuando el poderdante es una persona jurídica o ente sin personalidad, el órgano competente de los trámites objeto del apoderamiento, solicitará, en su caso, informe a su Asesoría Jurídica sobre la suficiencia de los poderes y demás documentos justificativos de la personalidad o de la representación. La inscripción del apoderamiento en el Registro o la eventual solicitud de subsanación de defectos en la representación al interesado, será llevada a cabo por el organismo competente. Si la subsanación no es atendida en un plazo máximo de diez días, se comunicará al interesado la imposibilidad de continuar el procedimiento, y la posibilidad de interponer el recurso previsto en artículo 29.2 del Reglamento del Servicio Jurídico del Estado, aprobado por el Real Decreto 997/2003, de 25 de julio.

Artículo 6. *Contenido del Registro electrónico de apoderamientos.*

1. Los apoderamientos dados de alta en el Registro sólo surtirán efecto respecto de las actuaciones o categorías a las que expresamente se refiera el apoderamiento otorgado, y hayan sido consignadas en el correspondiente formulario, de entre las que en cada momento se encuentren incorporadas al conjunto de trámites y actuaciones por medios electrónicos del Registro.

2. El Registro electrónico de apoderamientos estará disponible en la sede electrónica del punto de acceso general de la Administración General del Estado (https://sede.060.gob.es), donde se mantendrá una relación pública de todos los trámites y actuaciones por medios electrónicos de los departamentos ministeriales u organismos públicos adheridos al Registro, que pueden ser objeto de apoderamiento. Respecto de cada uno de los trámites que figuren en dicha relación se harán constar los datos que se aportaron para su inscripción en el Registro, a tenor de lo dispuesto en el artículo 9.

3. Para inscribir un apoderamiento en el Registro se harán constar los siguientes datos:

a) Nombre y apellidos, denominación o razón social y NIF del poderdante (o, en su defecto, documento equivalente).

b) Nombre y apellidos, denominación o razón social y NIF del apoderado (o, en su defecto, documento equivalente).

c) Trámites y actuaciones por medios electrónicos o categorías objeto de apoderamiento.

d) Periodo de vigencia del poder.

e) Fecha de otorgamiento.

f) Número de referencia del alta y fecha de alta en el Registro.

Artículo 7. *Renuncia y revocación del apoderamiento.*

La renuncia del apoderado a un apoderamiento inscrito en el Registro que regula esta Orden, o la revocación del mismo por el poderdante, surtirá efectos desde la comunicación fehaciente al órgano u organismo competente. La revocación y la renuncia podrán realizarse, utilizando los formularios previstos en los anexos II y III de esta Orden, por los mismos medios previstos en el artículo 3. La comprobación de la renuncia o revocación se hará de acuerdo con lo previsto en el artículo 5.

Artículo 8. *Trámites y actuaciones por medios electrónicos y sus categorías.*

1. En los supuestos en los que sea legalmente posible, y así lo determine el departamento ministerial u organismo competente sobre los trámites y actuaciones electrónicas objeto de apoderamiento, éste podrá establecer agrupaciones de trámites en categorías a las que podrán referirse los apoderamientos.

2. La categorización de los trámites será responsabilidad del organismo que se adhiera al Registro y, como mínimo, deberán diferenciarse los trámites que impliquen la consulta de datos personales y los trámites de recepción de notificaciones.

Artículo 9. *Adhesión al Registro electrónico de apoderamientos.*

1. La adhesión de un departamento ministerial u organismo público al Registro se llevará a efecto mediante la publicación en el «Boletín Oficial del Estado» de una Resolución del titular de la Subsecretaría del departamento o del titular del organismo. En dicha Resolución se concretarán además los trámites y actuaciones iniciales por medios electrónicos para los que será válida la representación incorporada al Registro electrónico de apoderamientos.

2. En la Resolución a que se refiere el apartado anterior se indicará para cada uno de los trámites y actuaciones por medios electrónicos referenciados:

a) El código y denominación del trámite, en su caso según la base de datos de procedimientos administrativos del Sistema de Información Administrativa, regulado en el Real Decreto-ley 8/2011, de 1 de julio, de medidas de apoyo a los deudores hipotecarios, de control del gasto público y cancelación de deudas con empresas y autónomos contraídas por las entidades locales, de fomento de la actividad empresarial e impulso de la rehabilitación y de simplificación administrativa.

b) La categoría a la que pertenece, de entre las definidas con anterioridad por el departamento ministerial, si procede.

c) El periodo máximo de vigencia de los apoderamientos para este trámite, que no podrá superar los 5 años.

d) En su caso, la necesidad de confirmación por el apoderado, para su eficacia.

e) La unicidad del apoderamiento. Se indicará si, para dicho trámite o actuación por medios electrónicos, un poderdante sólo puede inscribir a un apoderado en el Registro.

3. La incorporación posterior al Registro de nuevos trámites y actuaciones por medios electrónicos, y su eventual modificación corresponderá al departamento ministerial u organismo competente sobre los mismos. Esta incorporación se hará electrónicamente y deberá estar acompañada de una nueva Resolución del órgano competente modificando o ampliando la relación inicial de trámites.

4. En la sede electrónica de cada departamento ministerial u organismo público se relacionarán los trámites y actuaciones por medios electrónicos de su ámbito para los que se reconocen los apoderamientos inscritos en el Registro. Se resaltarán, además, en dicha sede las incorporaciones de nuevos trámites al Registro.

5. Aquellos departamentos ministeriales u organismos públicos que gestionen un Registro de apoderamientos propio, de ámbito limitado a trámites y actuaciones por medios electrónicos de su competencia no deberán inscribir éstos en el Registro electrónico de apoderamientos que regula esta Orden. No obstante, los organismos que gestionen un registro de apoderamientos propio podrán adherirse al Registro que regula esta Orden para la inscripción de trámites diferentes a los gestionados por su registro.

Artículo 10. *Consultas y certificaciones para el interesado.*

1. El Registro electrónico de apoderamientos no tiene carácter público, por lo que el interesado sólo podrá acceder, en aplicación del artículo 35 de la Ley 30/1992, de 26 de noviembre, a la información de los apoderamientos de los que sea poderdante o apoderado.

2. Las consultas y certificaciones podrán obtenerse por medios electrónicos, para lo cual el interesado podrá identificarse con los sistemas de identificación y autenticación previstos en el artículo 13.2.a) y b) de la Ley 11/2007, de 22 de junio. Estas opciones estarán disponibles en la sede electrónica del Punto de Acceso General de la Administración General del Estado (https://sede.060.gob.es). Las consultas y certificaciones serán firmadas con un certificado de sello electrónico. Además las consultas y certificaciones emitidas incluirán un Código Seguro de Verificación vinculado a la Secretaría de Estado de Administraciones Públicas, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica del Punto de Acceso General de la Administración General del Estado (https://sede.060.gob.es).

Artículo 11. *Acceso electrónico al Registro por la Administración General del Estado y sus organismos públicos.*

El Registro ofrecerá los siguientes procedimientos de acceso a la información a los departamentos ministeriales y organismos públicos adheridos al mismo:

a) Descarga bajo petición de un fichero, que contendrá todos los apoderamientos vigentes y válidos para los trámites y actuaciones por medios electrónicos de los que el órgano peticionario sea competente. El fichero contendrá todos los datos de los apoderamientos que se enumeran en el artículo 8.

b) Acceso en línea mediante servicios web, a los efectos de comprobar automáticamente y en tiempo real desde las aplicaciones que un apoderamiento está vigente. Las peticiones al Registro, relativas a los apoderamientos vigentes y válidos para los trámites y actuaciones por medios electrónicos de las que el órgano peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con un certificado de componente o de sello electrónico del citado órgano. La aplicación de soporte al Registro mantendrá traza de todas las peticiones recibidas.

Artículo 12. *Protección de Datos de Carácter Personal.*

Con la finalidad de dar cumplimiento a lo establecido en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, cuando el poderdante o el apoderado fueran persona física, deberá constar su consentimiento al tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del Registro de apoderamientos. Este consentimiento, que no será necesario reiterar para cada apoderamiento, dejará a salvo el ejercicio de los derechos de acceso, rectificación y cancelación establecidos en la citada Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 13. *Fichero de Protección de Datos.*

(Derogado)

Disposición adicional primera. *Adhesión al Registro.*

El ámbito de aplicación previsto en el artículo 1 de esta Orden podrá extenderse a otras Administraciones Públicas, mediante la formalización de un convenio al efecto con el Ministerio de Hacienda y Administraciones Públicas.

Disposición adicional segunda. *No incremento de gasto público.*

La constitución y funcionamiento del registro se atenderán con los medios personales y materiales existentes en el Ministerio de Hacienda y Administraciones Públicas, y en ningún caso podrá generar incremento de gasto público.

Disposición final primera. *Modificación de formularios.*

Corresponde a la Secretaría de Estado de Administraciones Públicas la modificación de los formularios para la inscripción en el Registro, que se incluye en el anexo I de la presente Orden, para la revocación de poderes, que se incluye en el Anexo II, para la renuncia de apoderamientos, que se incluye en el anexo III, así como la aprobación de otros formularios que, en su caso, resulten precisos para la gestión de dicho Registro.

Disposición final segunda. *Entrada en vigor.*

La presente Orden entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado».

ANEXO I

ANEXO I

INSCRIPCION EN EL REGISTRO ELECTRONICO DE APODERAMIENTOS PARA LA REALIZACION DE TRÁMITES Y ACTUACIONES POR MEDIOS ELECTRÓNICOS, MEDIANTE COMPARECENCIA DEL PODERDANTE O MEDIANTE PODER OTORGADO POR DOCUMENTO PÚBLICO O PRIVADO NOTARIALMENTE LEGITIMADO

D/Dª (nombre y dos apellidos) (*).....

con NIF/NIE (*) .....

☐ en nombre propio

☐ como representante según documento justificativo que se adjunta (1) del interesado:

☐ Nombre del interesado persona jurídica (razón social).....con NIF.....

☐ Nombre del interesado persona física.....con NIF.....

OTORGA SU REPRESENTACIÓN A:

D/Dª (nombre y dos apellidos)(*)..... NIF/NIE(*).....

en representación de la entidad (razón social) .....NIF .....

PARA LA REALIZACIÓN DE LOS SIGUIENTES TRÁMITES Y ACTUACIONES POR MEDIOS ELECTRÓNICOS DE LOS ESPECIFICADOS EN LA SEDE ELECTRÓNICA DEL PUNTO DE ACCESO GENERAL DE LA ADMINISTRACIÓN GENERAL DEL ESTADO (https://sede.060.gob.es):

CODIGO	CATEGORIA	DESCRIPCION	PERIODO DE VIGENCIA

El poderdante y apoderado (2) autorizan a que sus datos personales sean tratados de manera automatizada a los exclusivos efectos de los trámites y actuaciones por medios electrónicos objeto de la representación.
En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos de que sus datos personales serán incorporados a un fichero cuyo titular será la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, pudiendo ejercer los derechos de acceso, rectificación, cancelación y oposición en:

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica
Ministerio de Hacienda y Administraciones Públicas
C/ María de Molina, 50 - 28071 - MADRID
Correo electrónico: sgprotec@seap.minhap.es

En caso de apoderamientos otorgados mediante documento público o privado con firma legitimada notarialmente, deben hacerse constar los siguientes datos:

- NOTARIO O FEDATARIO PÚBLICO Y COLEGIO:
- NÚMERO DE PROTOCOLO:
- FECHA DEL DOCUMENTO DE REPRESENTACIÓN:

ACEPTACIÓN DE LA REPRESENTACIÓN (2).

Con la firma del presente escrito el apoderado acepta la representación conferida.

NORMAS APLICABLES

....

En ..... a ..... de ..... de.....

EL OTORGANTE EL APODERADO(2) EL FUNCIONARIO (Número de Registro de Personal)

(1) Si se trata de un representante legal, copia fidedigna de la escritura o documento constitutivo de la persona jurídica o entidad y documento público de su nombramiento de cargo o administrador, vigentes e inscritos en los Registros públicos correspondientes cuando procediere. En otro caso, documento público o privado con firma notarialmente legitimada que acredite poder suficiente para otorgar los apoderamientos de que se trate.

(2) Sólo cuando así lo requiera el trámite o actuación administrativa por medios electrónicos.

(*) campo obligatorio

NOTA: Este formulario está disponible en la sede electrónica del Punto de Acceso General de la Administración General del Estado: https://sede.060.gob.es

ANEXO II

ANEXO II

REVOCACIÓN DE APODERAMIENTOS EN EL REGISTRO ELECTRÓNICO DE APODERAMIENTOS PARA LA REALIZACIÓN DE TRÁMITES Y ACTUACIONES POR MEDIOS ELECTRÓNICOS, MEDIANTE COMPARECENCIA DEL PODERDANTE O MEDIANTE PODER OTORGADO POR DOCUMENTO PÚBLICO O PRIVADO NOTARIALMENTE LEGITIMADO

D/Dª (nombre y dos apellidos) (*).....

con NIF/NIE (*) .....

☐ en nombre propio

☐ como representante según documento justificativo que se adjunta (1), de la empresa (razón social).....con NIF.....

REVOCA LA REPRESENTACIÓN OTORGADA A:

D/Dª (nombre y dos apellidos)(*)..... NIF/NIE (*).....

en representación de la entidad (razón social) .....NIF .....

PARA LA REALIZACIÓN DE LOS SIGUIENTES TRÁMITES Y ACTUACIONES POR MEDIOS ELECTRÓNICOS DE LOS ESPECIFICADOS EN LA SEDE ELECTRÓNICA DEL SEDE ELECTRÓNICA DEL PUNTO DE ACCESO GENERAL DE LA ADMINISTRACIÓN GENERAL DEL ESTADO (https://sede.060.gob.es):

CODIGO	DESCRIPCION

En caso de apoderamientos otorgados mediante documento público o privado con firma legitimada notarialmente, deben hacerse constar los siguientes datos:

- NOTARIO O FEDATARIO PÚBLICO Y COLEGIO:
- NÚMERO DE PROTOCOLO:
- FECHA DEL DOCUMENTO DE REPRESENTACIÓN:

NORMAS APLICABLES

.....

En ..... a ..... de ..... de..... (*)

EL OTORGANTE EL FUNCIONARIO (Número de Registro de Personal)

(1) Si se trata de un representante legal, copia fidedigna de la escritura o documento constitutivo de la persona jurídica o entidad y documento público de su nombramiento de cargo o administrador, vigentes e inscritos en los Registros públicos correspondientes cuando procediere. En otro caso, documento público o privado con firma notarialmente legitimada que acredite poder suficiente para otorgar los apoderamientos de que se trate.

(*) campo obligatorio

NOTA: Este formulario está disponible en la sede electrónica del Punto de Acceso General de la Administración General del Estado: https://sede.060.gob.es

ANEXO III

ANEXO III

RENUNCIA DE APODERAMIENTOS EN EL REGISTRO ELECTRÓNICO DE APODERAMIENTOS PARA LA REALIZACIÓN DE TRÁMITES Y ACTUACIONES POR MEDIOS ELECTRÓNICOS, MEDIANTE COMPARECENCIA DEL APODERADO

D/Dª (nombre y dos apellidos)(*)..... NIF/NIE (*).....

en representación de la entidad (razón social) .....NIF .....

según documento justificativo que se adjunta (1)

RENUNCIA A LA REPRESENTACIÓN DE:

☐ la persona física (nombre y dos apellidos).....NIF/NIE.....

☐ la persona jurídica o ente sin personalidad (razón social).....con NIF.....

PARA LA REALIZACIÓN EN SU NOMBRE DE LOS SIGUIENTES TRÁMITES Y ACTUACIONES POR MEDIOS ELECTRÓNICOS DE LOS ESPECIFICADOS EN LA SEDE ELECTRÓNICA DEL PUNTO DE ACCESO GENERAL DE LA ADMINISTRACIÓN GENERAL DEL ESTADO (https://sede.060.gob.es):

CODIGO	DESCRIPCION

NORMAS APLICABLES

.....

En ..... a ..... de ..... de.....

EL APODERADO EL FUNCIONARIO (Número de Registro de Personal)

(1) Si se trata de un representante legal, copia fidedigna de la escritura o documento constitutivo de la persona jurídica o entidad y documento público de su nombramiento de cargo o administrador, vigentes e inscritos en los Registros públicos correspondientes cuando procediere. En otro caso, documento público o privado con firma notarialmente legitimada que acredite poder suficiente para otorgar los apoderamientos de que se trate.

(*) campo obligatorio.

NOTA: Este formulario está disponible en la sede electrónica del Punto de Acceso General de la Administración General del Estado: https://sede.060.gob.es

ANEXO IV

(Derogado)

§ 7

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: sin modificaciones
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, que será correlativo desde el comienzo de cada año.

3. En el pie de la página final de cada disposición, acto o anuncio se incluirá la dirección de la sede electrónica y el código de verificación que permita contrastar su autenticidad.
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 un sumario de su contenido.
6. Todas las disposiciones, actos y anuncios abrirán página y figurarán numerados de modo correlativo desde el comienzo de cada año.

Artículo 5. *Competencias.*

1. Corresponde al Ministerio de la Presidencia, a través de la Dirección General del 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.

2. Existirá asimismo un suplemento independiente en el que se publicarán las sentencias, declaraciones y autos del Tribunal Constitucional en los términos previstos en su ley orgánica.

Artículo 8. *Secciones.*

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 los edictos, notificaciones, requisitorias y anuncios de los Juzgados y Tribunales.
5. En la sección V se insertarán los anuncios, agrupados de la siguiente forma:

a) Anuncios de licitaciones públicas y adjudicaciones.
b) Otros anuncios oficiales.
c) Anuncios particulares.

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.

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 Dirección General del 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.

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.

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.

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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

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.

Artículo 20. *Remisión de documentos.*

Los originales destinados a la publicación en el «Boletín Oficial del Estado», se remitirán en formato electrónico y, excepcionalmente, en formato de papel, 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.

El formato de los documentos, ya sea de texto, gráfico, de imagen o cualquier otro, deberá ser susceptible de digitalización 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,y III, se aplicarán las siguientes normas:

a) La autenticidad de los originales remitidos para publicación habrá de quedar garantizada mediante su firma digital o, excepcionalmente, manuscrita, 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 Dirección General del Secretariado del Gobierno existirán los registros de firmas digitales o, en su caso, manuscritas 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 20.

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.

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 y III del «Boletín Oficial del Estado» serán remitidos, en todo caso, a la Dirección General del 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 Estado.

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 el suplemento correspondiente al Tribunal Constitucional se publicarán en forma íntegra.

2. Las resoluciones y actos comprendidos en las secciones II, III, IV y V se publicarán en extracto, siempre que sea posible y se reúnan los requisitos exigidos en cada caso.

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:

1. Se corregirán de oficio los errores de composición que se produzcan en la publicación, siempre que supongan alteración o modificación del sentido de las mismas o puedan suscitar dudas al respeto. A tal efecto, los correspondientes servicios de Dirección General del Secretariado del Gobierno y la Agencia Estatal Boletín Oficial del Estado, conservarán los originales de cada número, durante el plazo de seis meses, a partir de la fecha de su publicación.

2. Cuando se trate de errores padecidos en el texto remitido para publicación, su rectificación se realizará del modo siguiente:

a) 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.

b) 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, y actos de inserción obligatoria que deban ser incluidos en las secciones I, II y III se efectuará sin contraprestación económica por parte de los órganos que la hayan interesado.

2. La publicación de anuncios 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 del Estatuto de la Agencia Estatal Boletín Oficial del Estado aprobado por Real Decreto 1495/2007, de 12 de noviembre.

Disposición transitoria única. *Remisión telemática.*

1. De conformidad con el artículo 20, las disposiciones y actos de los departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado» se remitirán con arreglo a lo previsto en la Orden PRE/1563/2006, de 19 de mayo.

2. En tanto no se aprueben las restantes órdenes ministeriales previstas en el artículo 20, continuarán remitiéndose los originales a publicar en formato de 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.

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.*

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».

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día 1 de enero de 2009.

§ 8

Orden 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»

Ministerio de la Presidencia
«BOE» núm. 123, de 24 de mayo de 2006
Última modificación: 11 de abril de 2008
Referencia: BOE-A-2006-9004

El procedimiento de publicación de disposiciones y actos de inserción obligatoria en el «Boletín Oficial del Estado» se encuentra regulado por el Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado. Aunque su artículo 15 prevé que los textos a publicar pueden presentarse en soportes técnicos distintos del papel, o transmitirse directamente de acuerdo con las garantías y especificaciones que se determinen, hasta ahora este procedimiento se ha configurado exclusivamente sobre el envío de disposiciones en soporte papel que en todo caso debe incorporar, como garantía de su autenticidad, firma autógrafa de la autoridad o funcionario autorizado al efecto.

Dadas las peculiaridades del procedimiento de publicación de disposiciones, la sustitución de documentos en soporte papel por documentos electrónicos ha de realizarse sin menoscabo de su principio rector que es el de velar, en todas y en cada una de sus fases de tramitación, por la correcta y fiel publicación de las disposiciones y actos administrativos que deben insertarse en el «Boletín Oficial del Estado», garantizando su autenticidad, la reserva sobre su contenido así como la competencia de la autoridad que ordena la inserción.

En el momento presente es posible automatizar con ese nivel de garantía el procedimiento de publicación de las disposiciones y actos administrativos de los departamentos ministeriales, agilizando las comunicaciones y los intercambios de documentación entre todos los sujetos participantes: los ministerios emisores de las disposiciones, la Dirección General del Secretariado del Gobierno, competente para la ordenación y control de su publicación y el organismo autónomo Boletín Oficial del Estado, al que corresponden las labores de impresión, distribución y venta del diario oficial.

El artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece, en su apartado 1, que las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias, y dispone, en su apartado 4, que los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características.

A su vez, el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, desarrolla el artículo 45 de la citada Ley 30/1992 con la pretensión de delimitar, en el ámbito de la Administración General del Estado, las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas.

La disposición adicional primera del Real Decreto 1229/2001, de 8 de noviembre, por el que se aprueba el Estatuto del organismo autónomo Boletín Oficial del Estado, habilita al titular del Ministerio de la Presidencia para establecer 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.

En su virtud, previa aprobación del Ministro de Administraciones Públicas, dispongo:

Artículo 1. *Objeto.*

Esta orden tiene por objeto establecer el procedimiento de remisión telemática de las disposiciones y actos administrativos de los distintos departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado».

Artículo 2. *Ámbito de aplicación.*

La presente orden es de aplicación a todas aquellas disposiciones y actos administrativos de los departamentos ministeriales y sus organismos adscritos que no adopten la forma de real decreto y deban publicarse, de conformidad con lo previsto por el Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado, en las secciones I, II y III del «Boletín Oficial del Estado».

Artículo 3. *Registro de firmas digitales.*

Sin perjuicio de lo previsto en el artículo 14 del Real Decreto 1511/1986, de 6 de junio, a fin de comprobar la autenticidad de los documentos electrónicos remitidos, la Dirección General del Secretariado del Gobierno llevará un registro de las firmas digitales de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

A tal efecto, los titulares de firma de inserción deberán contar con un certificado de clase 2CA expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

La Dirección General del Secretariado del Gobierno, competente para la ordenación y control de la publicación de las disposiciones y actos administrativos que deban insertarse en el «Boletín Oficial del Estado», comprobará la autenticidad e integridad de firmas electrónicas remitidas, así como el cumplimiento de los requisitos formales necesarios en cada caso.

Artículo 4. *Aprobación de la aplicación informática «Insértese digital».*

Los textos electrónicos de las disposiciones y actos administrativos de los departamentos ministeriales se remitirán a la Dirección General del Secretariado del Gobierno a través de la aplicación informática «Insértese digital» cuyas características figuran en el anexo de esta orden.

La aplicación informática «Insértese digital» es conforme con los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» publicados por Resolución de la Secretaría de Estado para la Administración Pública, de 26 de mayo de 2003.

Artículo 5. *Conservación de originales electrónicos.*

Sin perjuicio de la conservación de originales que corresponde realizar a los servicios de la Dirección General del Boletín Oficial del Estado, a efectos de lo previsto en el artículo 19 del Real Decreto 1511/1986, de 6 de junio, la Dirección General del Secretariado del Gobierno conservará, mediante un sistema de archivo que permita la consulta posterior y la prueba de su integridad, tanto el texto de los originales electrónicos remitidos como el de las

firmas asociadas a ellos, así como el mecanismo de firma y la clave pública de la persona que ha firmado.

La conservación de originales electrónicos se realizará de conformidad con los requisitos recogidos en los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» publicados por Resolución de la Secretaría de Estado para la Administración Pública, de 26 de mayo de 2003.

Artículo 6. *Remisión al organismo autónomo Boletín Oficial del Estado.*

La Dirección General del Secretariado del Gobierno remitirá al organismo autónomo Boletín Oficial del Estado los textos electrónicos de las disposiciones y actos administrativos firmados digitalmente. A tal efecto, este organismo llevará un registro de las firmas digitales de las autoridades y funcionarios de la Dirección General del Secretariado del Gobierno facultados para la remisión.

Artículo 7. *Instrucciones complementarias.*

La Subsecretaría de la Presidencia establecerá las instrucciones a las que deberán ajustarse los departamentos ministeriales para la remisión telemática de los originales electrónicos.

Artículo 8. *Entrada en vigor.*

Lo dispuesto en esta orden entrará en vigor el día 1 de junio de 2006.

ANEXO

Características de la aplicación informática «Insértese digital»

1. Objeto: la aplicación «Insértese digital» tiene por objeto posibilitar la remisión telemática a la Dirección General del Secretariado del Gobierno de las disposiciones y actos administrativos de los distintos departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado».

2. Funcionalidad: la aplicación «Insértese digital» ofrece las siguientes utilidades:

Firma electrónica de documentos empleando certificados de clase 2CA expedidos por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Transmisión telemática de los documentos firmados a la Dirección General del Secretariado del Gobierno del Ministerio de la Presidencia.

Verificación de la autenticidad e integridad de los documentos electrónicos recibidos y de sus firmas.

3. Órgano competente: Dirección General del Secretariado del Gobierno, conforme a lo previsto por el artículo 6.1 e) del Real Decreto 1418/2004, de 11 de junio, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia.

4. Usuarios de la aplicación:

Usuarios titulares de insértese, facultados para firmar la inserción de los documentos electrónicos destinados a publicación.

Usuarios tramitadores, facultados para remitir telemáticamente los documentos electrónicos firmados.

Los usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos de utilización personal necesarios para su autenticación en el acceso al sistema, el establecimiento de la conexión precisa y, en su caso, la utilización de firma electrónica.

5. Medios de acceso: el acceso a la aplicación se realizará a través de la intranet del Ministerio de la Presidencia, para lo cual deberá disponerse de una identificación de usuario y de la correspondiente clave de acceso.

§ 9

Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad

Ministerio de la Presidencia
«BOE» núm. 310, de 28 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-22786

Actualmente, en la mayoría de las relaciones de los ciudadanos con la Administración éstos deben presentar una fotocopia de su documento de identidad, ya sea su DNI, si se trata de un ciudadano español o su tarjeta equivalente para el caso de extranjeros residentes en territorio español.

Se estima que el número de fotocopias de documentos acreditativos de la identidad de un ciudadano presentadas anualmente en los trámites administrativos asciende a más de cuatro millones.

El 28 de abril de 2006, el Consejo de Ministros aprobó el Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

Los objetivos de dicha norma son, por un lado, suprimir la obligación de presentar fotocopias de los documentos acreditativos de identidad en todos los trámites administrativos, pudiendo sustituirse dicha fotocopia, en aquellos supuestos donde la constancia de los datos fuese imprescindible, por una consulta telemática a la Dirección General de la Policía y de la Guardia Civil de forma directa o diferida; y por otro dotar de mayor seguridad al método actual de verificación de la identidad de un ciudadano, ya que es más fácil manipular una fotocopia que suplantar la identidad del sistema de verificación de datos de identidad basado en la información preservada por la Dirección General de la Policía y de la Guardia Civil.

A partir de la puesta en funcionamiento de este sistema es el propio Departamento ante el que se solicita el trámite el encargado de comprobar, de oficio, la identidad del interesado. Esta consulta se realizará, en los casos en los que sea estrictamente necesario y tras obtener la autorización del interesado. La consulta se realizará con máximas garantías de seguridad y preservando la privacidad de los datos. En caso de que el interesado no dé su consentimiento a realizar esa consulta, deberá aportar su correspondiente fotocopia del Documento Nacional de Identidad.

El objeto de la presente Orden Ministerial es dar cumplimiento al mandato contenido en la disposición final primera del citado Real Decreto 522/2006, de 28 de abril, en virtud del cual el establecimiento de la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad, así como la fecha en que dicho

sistema estará plenamente operativo, se llevará a cabo mediante orden, a propuesta conjunta de los Ministros del Interior y de Administraciones Públicas.

A tal fin, se han tenido en consideración las experiencias previas, las implicaciones técnicas, la búsqueda de racionalidad y sencillez de uso y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo respectivos informes favorables del Consejo Superior de Administración Electrónica y de la Agencia de Protección de Datos, a propuesta de los Ministros del Interior y de Administraciones Públicas, dispongo:

Primero.

Se aprueba el Reglamento Técnico del Sistema de Verificación de Datos de Identidad, que figura como anexo a la presente Orden Ministerial, como instrumento que establece la configuración, características, requisitos y procedimientos de acceso al citado Sistema.

Segundo.

Se fija como fecha de operatividad del Sistema de Verificación de Datos de Identidad el uno de enero de 2007, a partir de la cual no podrá exigirse por la Administración General del Estado o por los Organismos vinculados o dependientes de aquella la aportación de fotocopias del Documento Nacional de Identidad o de los documentos acreditativos de la identidad de extranjeros residentes en España o tarjeta equivalente, salvo en los supuestos previstos en el Real Decreto 522/2006, de 28 de abril.

Tercero.

La presente Orden Ministerial se aprueba en aplicación de lo dispuesto en la disposición final primera del Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

Disposición final primera. *Aplicación y desarrollo.*

1. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio del Interior y previo informe del Consejo Superior de Administración Electrónica, se establecerán los parámetros de calidad de la prestación del servicio del Sistema de Verificación de Datos de Identidad y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial. A estos efectos, el Ministerio de Administraciones Públicas establecerá instrumentos de validación y vigilancia del cumplimiento de lo establecido en el párrafo anterior, sin perjuicio de las competencias de los Órganos de Control Interno.

2. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio del Interior y previo informe del Consejo Superior de Administración Electrónica, se podrá proceder a la actualización o modificación del Reglamento Técnico que se aprueba por la presente Orden Ministerial.

3. Se faculta a los Subsecretarios de los departamentos Ministeriales, a los Presidentes de los Organismos Públicos o a los responsables ministeriales correspondientes, para la adopción de las instrucciones o medidas que resulten adecuadas para garantizar el acceso y la utilización del Sistema de Verificación de Datos de Identidad por los órganos y unidades correspondientes a su ámbito.

Disposición final segunda. *Entrada en vigor.*

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Reglamento Técnico del Sistema de Verificación de Datos de Identidad

Primero. *Descripción del Sistema de Verificación de Datos de Identidad.*

El Sistema de Verificación de Datos de Identidad puesto a disposición de los Departamentos y Organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos del Documento de Identificación del Ciudadano custodiados por la Dirección General de la Policía y de la Guardia Civil en base a lo dispuesto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que atribuye al Cuerpo Nacional de Policía, la función de expedición del Documento Nacional de Identidad y el control de entrada y salida del territorio nacional de españoles y extranjeros. Información que se encuentra registrada y custodiada en los ficheros de la Dirección General de la Policía y de la Guardia Civil, que soportan la gestión del documento nacional de identidad y la Tarjeta de Identificación de Extranjeros (Sus denominaciones, conforme a las Órdenes INT/1751/2002, de 20 de junio e INT/2190/2006, de 19 de junio, son ADDNIFIL y ADEXTTRA, respectivamente).

Segundo. *Adopción de medidas de seguridad, organizativas o técnicas de los organismos y aplicaciones que accedan al Sistema de Verificación de Datos de Identidad.*

1. Con carácter general los organismos que accedan al Sistema de Verificación de Datos de Identidad cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.

2. El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.

3. Lo dispuesto en esta Orden Ministerial se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 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.

Tercero. *Acceso al Sistema de Verificación de Datos de Identidad.*

1. El acceso al Sistema de Verificación de Datos de Identidad se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas, siguiendo el esquema de conexión que ésta tiene establecido para cualquier organismo público. Sólo en casos debidamente justificados y previa aprobación, por parte de la Secretaría del Consejo Superior de Administración Electrónica, de un plan para la ordenación de las comunicaciones se habilitarán temporalmente mecanismos de conexión alternativos.

2. El Sistema de Verificación de Datos de Identidad presentará dos formas alternativas de acceso para realizar las correspondientes consultas sobre la veracidad de ciertos datos de identidad:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto - HTTP/1.1 del IETF, donde un empleado público, debidamente acreditado e identificado, podrá realizar consultas con sólo disponer de un navegador con acceso al Sistema de Aplicaciones y Redes para las Administraciones Públicas y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los

Organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

Cuarto. *Requisitos de autenticidad para el acceso al Sistema de Verificación de Datos de Identidad.*

1. Los accesos al Sistema de Verificación de Datos de Identidad se efectuarán utilizando certificados electrónicos reconocidos.
2. Los certificados electrónicos que se utilicen para identificarse ante el Sistema de Verificación de Datos de Identidad deberán ser certificados reconocidos que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997).
3. No podrán utilizarse certificados electrónicos caducados o revocados para acceder al Sistema de Verificación de Datos de Identidad.

Quinto. *Requisitos de confidencialidad del Sistema de Verificación de Datos de Identidad.*

1. El Sistema de Verificación de Datos de Identidad ofrecerá consultas en las que, a partir del Número del Documento de Identificación del Ciudadano o Extranjero, se devolverá el total, o un subconjunto, de los datos incorporados en dicho documento:

Nombre y apellidos del titular del documento.
Lugar y fecha de nacimiento.
Nombre de los padres.
Sexo.
Estado de vigencia del Documento.

El conjunto de datos a los que tenga acceso cada usuario del sistema será establecido, previa autorización y justificación, por parte del responsable en la Organización Administrativa.

2. Sólo organismos públicos debidamente autorizados tendrán acceso al Sistema de Verificación de Datos de Identidad. En todo organismo público existirá un responsable o administrador delegado del sistema que autorizará los accesos al Sistema de Verificación de Datos de Identidad.
3. Para realizar la consulta al Sistema de Verificación de Datos de Identidad, será preciso el consentimiento del interesado cuyos datos se vayan a verificar, salvo que una norma con rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento.
4. La consulta y el acceso a la información proporcionada por el Sistema de Verificación de Datos de Identidad deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta.

Sexto. *Requisitos de integridad de la información proporcionada por el Sistema de Verificación de Datos de Identidad.*

Todas las consultas que se realicen al Sistema de Verificación de Datos de Identidad, así como las respuestas que devuelva el propio sistema, deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el Sistema de Verificación de Datos de Identidad deba realizar a la Dirección General de la Policía y de la Guardia Civil, así cómo las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad de ambos organismos.

Séptimo. *Requisitos de disponibilidad de la información proporcionada por el Sistema de Verificación de Datos de Identidad.*

El Sistema de Verificación de Datos de Identidad estará disponible los 7 días de la semana las 24 horas del día.

Octavo. *Garantías jurídicas del Sistema de Verificación de Datos de Identidad ante posibles recursos.*

1. El servicio web proporcionado por este sistema sigue el estándar de intercambio de datos definido por «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

2. El Sistema de Verificación de Datos de Identidad dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de identidad realizadas, información de contexto asociada, como la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

3. Para certificar la fecha y tiempo de las actividades y sucesos registrados en el Sistema de Verificación de Datos de Identidad se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada 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 el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

4. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría del Sistema de Verificación de Datos de Identidad.

Noveno. *Condiciones de la prestación del servicio.*

1. La gestión del Sistema de Verificación de Datos de Identidad corresponde al Ministerio de Administraciones Públicas.

2. Los organismos públicos que hagan uso de este servicio estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en esta Orden Ministerial.

3. Para poder acceder al Sistema de Verificación de Datos de Identidad, los Organismos Administrativos deberán designar a un responsable, tal y como se indica en el apartado segundo del punto quinto del presente anexo técnico, que será el encargado de autorizar a los accesos en su organismo. El nombramiento y cese de este responsable deberá ser comunicado al Ministerio de Administraciones Públicas, para la asignación de los permisos adecuados de acceso al sistema o la cancelación de los mismos.

§ 10

Orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia

Ministerio de la Presidencia
«BOE» núm. 1, de 1 de enero de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-1

Actualmente, en la mayoría de las relaciones de los ciudadanos con la Administración, éstos deben indicar su lugar de residencia con un nivel de rigurosidad que varía desde la declaración expresa hasta la presentación de un certificado de empadronamiento expedido por el municipio en el cual están registrados sus datos de empadronamiento.

Se estima que el número de documentos acreditativos de la residencia expedidos anualmente asciende a más de diez millones de los cuales más de tres millones han sido solicitados, a su vez, por la Administración.

El 28 de abril de 2006, el Consejo de Ministros aprobó el Real Decreto 523/2006, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

Los objetivos de dicha norma son, por un lado, no exigir a quien tenga la condición de interesado en los procedimientos cuya tramitación y resolución corresponda a la Administración General del Estado o a los organismos públicos vinculados o dependientes de aquélla, la aportación del certificado de empadronamiento como documento acreditativo del domicilio y residencia; y por otro sustituir, en los procedimientos para cuya tramitación sea imprescindible acreditar de modo fehaciente los datos del domicilio y residencia del interesado, la presentación de documento acreditativo por una consulta electrónica mediante un Sistema de Verificación de Datos de Residencia puesto a disposición de los organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas y el Instituto Nacional de Estadística dependiente del Ministerio de Economía y Hacienda.

A partir de la puesta en producción de este sistema es el propio Departamento ante el que se solicita el trámite el encargado de comprobar, de oficio, la residencia del interesado. Esta consulta se realizará, en los casos en los que sea estrictamente necesario y tras obtener la autorización del interesado. La consulta se realizará con máximas garantías de seguridad y preservando la privacidad de los datos. En caso de que el interesado no dé su consentimiento a realizar esa consulta, deberá aportar el documento acreditativo de residencia que estime apropiado el organismo tramitador del expediente.

La presente Orden Ministerial tiene por objeto dar cumplimiento al mandato señalado en el Real Decreto 523/2006 de 28 de abril. A tal fin, se han tenido en consideración las

experiencias previas, las implicaciones técnicas, la búsqueda de racionalidad y sencillez de uso y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo respectivos informes favorables del Consejo Superior de Administración Electrónica y de la Agencia Española de Protección de Datos, a propuesta de los Ministros de Economía y Hacienda y de Administraciones Públicas, dispongo:

Artículo único. *Objeto.*

1. Se aprueba el Reglamento Técnico del Sistema de Verificación de Datos de Residencia, que figura como anexo a la presente Orden Ministerial, como instrumento que establece la configuración, características, requisitos y procedimientos de acceso al citado Sistema.

2. Se fija como fecha de operatividad del Sistema de Verificación de Datos de Residencia la de entrada en vigor de la presente Orden, a partir de la cual no podrá exigirse en los procedimientos cuya tramitación y resolución corresponda a la Administración General del Estado, o a los Organismos vinculados o dependientes de aquélla, la aportación de certificados de empadronamiento, salvo en los supuestos previstos en el Real Decreto 523/2006, de 28 de abril.

3. La presente Orden Ministerial se aprueba en aplicación de lo dispuesto en la disposición final primera del Real Decreto 523/2006, de 28 de abril, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

Disposición final primera. *Aplicación y desarrollo.*

1. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio de Economía y Hacienda y previo informe del Consejo Superior de Administración Electrónica, se establecerán los parámetros de calidad de la prestación del servicio del Sistema de Verificación de Datos de Residencia y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial. A estos efectos, el Ministerio de Administraciones Públicas establecerá instrumentos de validación y vigilancia del cumplimiento de lo establecido en el párrafo anterior, sin perjuicio de las competencias de los Órganos de Control Interno.

2. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio de Economía y Hacienda y previo informe del Consejo Superior de Administración Electrónica, se podrá proceder a la actualización o modificación del Reglamento Técnico que se aprueba por la presente Orden Ministerial.

3. Se faculta a los Subsecretarios de los departamentos Ministeriales, a los Presidentes de los Organismos Públicos o a los responsables ministeriales correspondientes, para la adopción de las instrucciones o medidas que resulten adecuadas para garantizar el acceso y la utilización del Sistema de Verificación de Datos de Residencia por los órganos y unidades correspondientes a su ámbito.

Disposición final segunda. *Entrada en vigor.*

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Reglamento Técnico del Sistema de Verificación de Datos de Residencia

Primero. Descripción del Sistema de Verificación de Datos de Residencia.

El Sistema de Verificación de Datos de Residencia puesto a disposición de los Departamentos y Organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos sobre residencia de los ciudadanos mediante el acceso a los Padrones municipales coordinados por el Instituto Nacional de Estadística, en base a lo dispuesto en la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, en relación con el Padrón Municipal, en la que se atribuye al Instituto Nacional de Estadística, entre otras, la función de coordinación de los distintos padrones municipales. Ésta información se encuentra registrada y custodiada en los ficheros del Instituto Nacional de Estadística registrados en la Agencia de Protección de Datos con la denominación «PADRONES MUNICIPALES», conforme a la Orden ECO/143/2002, de 10 de enero, publicada en el BOE 26, de 30 de enero de 2002.

Segundo. Adopción de medidas de seguridad, organizativas o técnicas del acceso al Sistema de Verificación de Datos de Residencia.

1. Con carácter general los organismos que accedan al Sistema de Verificación de Datos de Residencia cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.

2. El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.

3. Lo dispuesto en esta Orden Ministerial se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia como 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.

Tercero. Acceso al Sistema de Verificación de Datos de Residencia.

1. El acceso al Sistema de Verificación de Datos de Residencia se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas, siguiendo el esquema de conexión que ésta tiene establecido para cualquier departamento u organismo público. Sólo en casos debidamente justificados y previa aprobación, por parte de la Secretaría del Consejo Superior de Administración Electrónica, de un plan para la ordenación de las comunicaciones se habilitarán temporalmente mecanismos de conexión alternativos.

2. El Sistema de Verificación de Datos de Residencia presentará dos formas de acceso para realizar las correspondientes consultas sobre el lugar de domicilio y residencia de un ciudadano:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto – HTTP/1.1 o superior, del IETF, donde un empleado público, debidamente acreditado e identificado, podrá realizar consultas con sólo disponer de un navegador con acceso al Sistema de Aplicaciones y Redes para las Administraciones Públicas y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los departamentos y organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

Cuarto. Requisitos de autenticidad para el acceso al Sistema de Verificación de Datos de Residencia.

1. Los accesos al Sistema de Verificación de Datos de Residencia se efectuarán utilizando certificados electrónicos reconocidos.

2. Los certificados electrónicos que se utilicen para identificarse ante el Sistema de Verificación de Datos de Residencia deberán ser certificados reconocidos que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997).

3. No podrán utilizarse certificados electrónicos caducados o revocados para acceder al Sistema de Verificación de Datos de Residencia.

Quinto. Requisitos de confidencialidad del Sistema de Verificación de Datos de Residencia.

1. El Sistema de Verificación de Datos de Residencia, a partir del Número del Documento de Identificación del Ciudadano y/o de un conjunto de datos personales suficientes para identificar unívocamente al mismo, devolverá el total, o un subconjunto de los datos referentes al domicilio y residencia asociados a un ciudadano:

Provincia.
Municipio.
Entidad Colectiva.
Entidad Singular.
Núcleo.
Dirección (Via, Kmt, Número, Número Superior, Bloque, Portal, Escalera, Planta, Puerta).

El conjunto de datos a los que tenga acceso cada usuario del sistema será establecido, previa autorización y justificación, por parte del responsable en la Organización Administrativa.

En caso de que los datos introducidos no fueran suficientes para identificar de manera única a un ciudadano el sistema no devolverá en la respuesta información sobre ningún ciudadano.

2. Sólo organismos públicos debidamente autorizados tendrán acceso al Sistema de Verificación de Datos de Residencia. En todo organismo público existirá un responsable o administrador delegado del sistema que autorizará los accesos al Sistema de Verificación de Datos de Residencia.

3. Para realizar la consulta al Sistema de Verificación de Datos de Residencia, será preciso el consentimiento del interesado cuyos datos se vayan a consultar, salvo que una norma de rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento.

4. La consulta y el acceso a la información proporcionada por el Sistema de Verificación de Datos de Residencia deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta.

Sexto. Requisitos de integridad de la información proporcionada por el Sistema de Verificación de Datos de Residencia.

Todas las consultas que se realicen al Sistema de Verificación de Datos de Residencia, así como las respuestas que devuelva el propio sistema, deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar tanto la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el Sistema de Verificación de Datos de Residencia deba realizar al Instituto Nacional de Estadística o a otros organismos con capacidad de informar sobre la residencia de los ciudadanos, así cómo las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad de ambos organismos.

Séptimo. Requisitos de disponibilidad de la información proporcionada por el Sistema de Verificación de Datos de Residencia.

El Sistema de Verificación de Datos de Residencia estará disponible los 7 días de la semana las 24 horas del día.

Octavo. Garantías jurídicas del Sistema de Verificación de Datos de Residencia ante posibles recursos.

1. El servicio web proporcionado por este sistema sigue el estándar de intercambio de datos definido por la iniciativa «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

2. El Sistema de Verificación de Datos de Residencia dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de residencia realizadas, información de contexto asociada, la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

3. Para certificar la fecha y tiempo de las actividades y sucesos registrados en el Sistema de Verificación de Datos de Residencia se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada 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 el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

4. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoria del Sistema de Verificación de Datos de Residencia.

Noveno. Condiciones de la prestación del servicio.

1. La gestión del Sistema de Verificación de Datos de Residencia corresponde al Ministerio de Administraciones Públicas.

2. Los organismos públicos que hagan uso de este servicio estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en esta Orden Ministerial.

3. Para poder acceder al Sistema de Verificación de Datos de Residencia, los Organismos Administrativos deberán designar a un responsable, tal y como se indica en el apartado segundo del punto quinto del presente anexo técnico, que será el encargado de autorizar los accesos en su organismo. El nombramiento y cese de este responsable deberá ser comunicado al Ministerio de Administraciones Públicas, para la asignación de los permisos adecuados de acceso al sistema o la cancelación de los mismos.

§ 11

Ley 59/2003, de 19 de diciembre, de firma electrónica

Jefatura del Estado
«BOE» núm. 304, de 20 de diciembre de 2003
Última modificación: 29 de diciembre de 2007
Referencia: BOE-A-2003-23399

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

El Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyuvaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado real decreto ley incorporó al ordenamiento público español 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, incluso antes de su promulgación y publicación en el Diario Oficial de las Comunidades Europeas.

Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto Ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando a la vez el marco establecido en el Real Decreto Ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

II

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Asimismo, debe destacarse que la ley define una clase particular de certificados electrónicos denominados certificados reconocidos, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

La certificación técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el "Diario Oficial de las Comunidades Europeas" o, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología.

Adicionalmente, la ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

III

Esta ley se promulga para reforzar el marco jurídico existente incorporando a su texto algunas novedades respecto del Real Decreto Ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

Así, se revisa la terminología, se modifica la sistemática y se simplifica el texto facilitando su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa.

Una de las novedades que la ley ofrece respecto del Real Decreto Ley 14/1999, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita. Se trata simplemente de la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto Ley 14/1999 venían exigiendo. Con ello se aclara que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación.

Asimismo, es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

Por otra parte, la ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación.

El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público.

Si bien se recogen fielmente en la ley los conceptos de "acreditación" de prestadores de servicios de certificación y de "conformidad" de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Otra modificación relevante es que la ley clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Por otra parte, dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

También ha de destacarse la regulación que la ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

Asimismo, otra novedad es el establecimiento en la ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático. Se va así más allá del Real Decreto Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos.

Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la ley exige, por un lado, una especial legitimación para que las personas físicas soliciten la expedición de certificados ; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Con la expresión "giro o tráfico ordinario" de una entidad se actualiza a un vocabulario más acorde con nuestros días lo que en la legislación mercantil española se denomina "establecimiento fabril o mercantil". Con ello se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. Por último, debe recalcarse que, aunque el "giro o tráfico ordinario" sea un término acuñado por el derecho mercantil, la regulación sobre los certificados de personas jurídicas no sólo se aplica a las sociedades mercantiles, sino a cualquier tipo de persona jurídica que quiera hacer uso de la firma electrónica en su actividad.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

Por otra parte, siguiendo la pauta marcada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Además, debe resaltarse que otro aspecto novedoso de la ley es el acogimiento explícito que se efectúa de las relaciones de representación que pueden subyacer en el empleo de la firma electrónica. No cabe duda que el instituto de la representación está ampliamente generalizado en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica.

Para ello, se establece como novedad que en la expedición de certificados reconocidos que admitan entre sus atributos relaciones de representación, ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante. Asimismo, se prevén mecanismos para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.

Por último, debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los

Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos.

Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores.

IV

La ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores -distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

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.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

2. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

Artículo 2. *Prestadores de servicios de certificación sujetos a la ley.*

1. Esta ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

2. Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

3. Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle 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.

4. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

5. Se presumirá que un prestador de servicios de certificación está establecido en España cuando dicho 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 mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

Artículo 3. *Firma electrónica, y documentos firmados electrónicamente.*

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la 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.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

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.

6. El documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

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.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

Artículo 4. *Empleo de la firma electrónica en el ámbito de las Administraciones públicas.*

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

2. Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto 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. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Artículo 5. *Régimen de prestación de los servicios de certificación.*

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

TÍTULO II

Certificados electrónicos

CAPÍTULO I

Disposiciones generales

Artículo 6. *Concepto de certificado electrónico y de firmante.*

1. Un certificado electrónico es un 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.

2. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Artículo 7. *Certificados electrónicos de personas jurídicas.*

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.

Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.

Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

5. Lo dispuesto en este artículo no será de aplicación a los certificados que sirvan para verificar la firma electrónica del prestador de servicios de certificación con la que firme los certificados electrónicos que expida.

6. Lo dispuesto en este artículo no será de aplicación a los certificados que se expidan a favor de las Administraciones públicas, que estarán sujetos a su normativa específica.

Artículo 8. *Extinción de la vigencia de los certificados electrónicos.*

1. Son causas de extinción de la vigencia de un certificado electrónico:

a) Expiración del período de validez que figura en el certificado.

b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

d) Resolución judicial o administrativa que lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del firmante ; fallecimiento, o extinción de la personalidad jurídica del representado ; incapacidad sobrevenida, total o parcial, del firmante o de su representado ; terminación de la representación ; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma.

En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

3. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 9. *Suspensión de la vigencia de los certificados electrónicos.*

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

b) Resolución judicial o administrativa que lo ordene.

c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.

d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 10. *Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos.*

1. El prestador de servicios de certificación hará constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

2. El prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

3. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

4. La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

CAPÍTULO II

Certificados reconocidos

Artículo 11. *Concepto y contenido de los certificados reconocidos.*

1. 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 presten.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

Artículo 12. *Obligaciones previas a la expedición de certificados reconocidos.*

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.

b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.

c) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Artículo 13. *Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido.*

1. La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

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.

4. Lo dispuesto en los apartados anteriores podrá no ser exigible en los siguientes casos:

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b) Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

5. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

Artículo 14. *Equivalencia internacional de certificados reconocidos.*

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b) Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPÍTULO III

El documento nacional de identidad electrónico

Artículo 15. *Documento nacional de identidad electrónico.*

1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Artículo 16. *Requisitos y características del documento nacional de identidad electrónico.*

1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

TÍTULO III

Prestación de servicios de certificación

CAPÍTULO I

Obligaciones

Artículo 17. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que

tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 18. *Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.*

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

6.º Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

Artículo 19. *Declaración de prácticas de certificación.*

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

Artículo 20. *Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.*

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.

b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.

f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

2. Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

Artículo 21. *Cese de la actividad de un prestador de servicios de certificación.*

1. El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas ; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia.

La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

2. El prestador de servicios de certificación que expida certificados electrónicos al público deberá comunicar al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia.

Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

3. Los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f). Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo.

CAPÍTULO II

Responsabilidad

Artículo 22. *Responsabilidad de los prestadores de servicios de certificación.*

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta ley.

La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

2. Si el prestador de servicios de certificación no cumpliera las obligaciones señaladas en los párrafos b) al d) del artículo 12 al garantizar un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, será responsable por los daños y perjuicios causados por el uso de dicho certificado.

3. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

4. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

5. La regulación contenida en esta ley sobre la responsabilidad del prestador de servicios de certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores.

Artículo 23. *Limitaciones de responsabilidad de los prestadores de servicios de certificación.*

1. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

a) No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.

b) La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.

e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

f) Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

2. En el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando ésta tenga conocimiento de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta ley.

3. Cuando el firmante sea una persona jurídica, el solicitante del certificado electrónico asumirá las obligaciones indicadas en el apartado 1.

4. El prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

a) Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

b) Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

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.

6. La exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia.

TÍTULO IV

Dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica

CAPÍTULO I

Dispositivos de firma electrónica

Artículo 24. *Dispositivos de creación de firma electrónica.*

1. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Artículo 25. *Dispositivos de verificación de firma electrónica.*

1. Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

3. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

d) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f) Que pueda detectarse cualquier cambio relativo a su seguridad.

4. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

CAPÍTULO II

Certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica

Artículo 26. *Certificación de prestadores de servicios de certificación.*

1. La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

2. La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.

4. La certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica.

Artículo 27. *Certificación de dispositivos seguros de creación de firma electrónica.*

1. La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea" y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.

4. Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.

Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma.

Artículo 28. *Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica.*

1. Se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea".

2. Se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo.

TÍTULO V

Supervisión y control

Artículo 29. *Supervisión y control.*

1. El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

2. El Ministerio de Ciencia y Tecnología realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos al Ministerio de Ciencia y Tecnología que realicen la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. El Ministerio de Ciencia y Tecnología podrá acordar las medidas apropiadas para el cumplimiento de esta ley y sus disposiciones de desarrollo.

4. El Ministerio de Ciencia y Tecnología podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de certificación que le asigna esta ley.

Artículo 30. *Deber de información y colaboración.*

1. Los prestadores de servicios de certificación, la entidad independiente de acreditación y los organismos de certificación tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de sus funciones.

En particular, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección 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. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas.

2. Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores y será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

3. Cuando, como consecuencia de una actuación inspectora, 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.

TÍTULO VI

Infracciones y sanciones

Artículo 31. *Infracciones.*

1. Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.

Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.

3. Son infracciones graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.

b) La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.

c) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.

d) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.

e) El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

f) La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.

g) El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.

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.

Artículo 32. *Sanciones.*

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa de 150.001 a 600.000 euros.

La comisión de dos o más infracciones muy graves en el plazo de tres años, podrá dar lugar, en función de los criterios de graduación del artículo siguiente, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros.

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional o en la página de inicio del sitio de internet del prestador y, en su caso, en el sitio de internet del Ministerio de Ciencia y Tecnología, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito.

Artículo 33. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

a) La existencia de intencionalidad o reiteración.

b) La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.

c) La naturaleza y cuantía de los perjuicios causados.

d) Plazo de tiempo durante el que se haya venido cometiendo la infracción e) El beneficio que haya reportado al infractor la comisión de la infracción.

f) Volumen de la facturación a que afecte la infracción cometida.

Artículo 34. *Medidas provisionales.*

1. En los procedimientos sancionadores por infracciones graves o muy graves el Ministerio de Ciencia y Tecnología podrá 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 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 de certificación 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) Advertencia 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.

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 a la protección de los datos personales, cuando éstos pudieran resultar afectados.

2. En los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el prestador de servicios de certificación que menoscaben seriamente la confianza de los usuarios en los servicios ofrecidos, el Ministerio de Ciencia y Tecnología podrá acordar la suspensión o pérdida de vigencia de los certificados afectados, incluso con carácter definitivo.

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 este 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 15 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 35. *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 36. *Competencia y procedimiento sancionador.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo.

Disposición adicional primera. *Fe pública y uso de firma electrónica.*

1. Lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley.

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

Disposición adicional segunda. *Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica.*

1. En el ámbito de la certificación de dispositivos de creación de firma, corresponderá al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología la imposición de sanciones por la comisión, por los organismos de certificación de dispositivos seguros de creación de firma electrónica o por la entidad que los acredite, de las infracciones graves previstas en los párrafos e), f) y g) del

apartado segundo del artículo 31 de la Ley 21/1992, de 16 de julio, de Industria, y de las infracciones leves indicadas en el párrafo a) del apartado 3 del artículo 31 de la citada ley que cometan en el ejercicio de actividades relacionadas con la certificación de firma electrónica.

2. Cuando dichas infracciones merezcan la calificación de infracciones muy graves, serán sancionadas por el Ministro de Ciencia y Tecnología.

Disposición adicional tercera. *Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias.*

Podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda.

Disposición adicional cuarta. *Prestación de servicios por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

Lo dispuesto en esta ley se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

Disposición adicional quinta. *Modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.*

Se añaden apartado doce al artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, con la siguiente redacción.

> "Doce. En el ejercicio de las funciones que le atribuye el presente artículo, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda estará exenta de la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la Ley 59/2003, de Firma Electrónica."

Disposición adicional sexta. *Régimen jurídico del documento nacional de identidad electrónico.*

1. Sin perjuicio de la aplicación de la normativa vigente en materia del documento nacional de identidad en todo aquello que se adecue a sus características particulares, el documento nacional de identidad electrónico se regirá por su normativa específica.

2. El Ministerio de Ciencia y Tecnología podrá dirigirse al Ministerio del Interior para que por parte de éste se adopten las medidas necesarias para asegurar el cumplimiento de las obligaciones que le incumban como prestador de servicios de certificación en relación con el documento nacional de identidad electrónico.

Disposición adicional séptima. *Emisión de facturas por vía electrónica.*

Lo dispuesto en esta ley se entiende sin perjuicio de las exigencias derivadas de las normas tributarias en materia de emisión de facturas por vía electrónica.

Disposición adicional octava. *Modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

Uno. Adición de un nuevo apartado 3 al artículo 10 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Se añade un apartado 3 con el siguiente texto:

> "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."

Dos. Los apartados 2, 3 y 4 del artículo 38 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se redactan en los siguientes términos:

"2. Son infracciones muy graves:

a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

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) El incumplimiento significativo de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.

d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

a) El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.

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 el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, 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) El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22.

4. Son infracciones leves:

a) La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.

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) El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.

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."

Tres. Modificación del artículo 43, apartado 1, segundo párrafo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El segundo párrafo del apartado 1 del artículo 43 queda redactado como sigue:

"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."

Cuatro. Modificación del artículo 43, apartado 2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El apartado 2 del artículo 43 queda redactado como sigue:

"2. 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."

Disposición adicional novena. *Garantía de accesibilidad para las personas con discapacidad y de la tercera edad.*

Los servicios, procesos, procedimientos y dispositivos de firma electrónica deberán ser plenamente accesibles a las personas con discapacidad y de la tercera edad, las cuales no podrán ser en ningún caso discriminadas en el ejercicio de los derechos y facultades reconocidos en esta ley por causas basadas en razones de discapacidad o edad avanzada.

Disposición adicional décima. *Modificación de la Ley de Enjuiciamiento Civil.*

Se añade un apartado tres al artículo 326 de la Ley de Enjuiciamiento Civil con el siguiente tenor:

> "Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica."

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.

Disposición transitoria primera. *Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta ley.*

Los certificados electrónicos que hayan sido expedidos por prestadores de servicios de certificación en el marco del Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, mantendrán su validez.

Disposición transitoria segunda. *Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley.*

Los prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley deberán comunicar al Ministerio de Ciencia y Tecnología su actividad y las características de los servicios que presten en el plazo de un mes desde la referida entrada en vigor. Esta información será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley.

Disposición final primera. *Fundamento constitucional.*

Esta ley se dicta al amparo del artículo 149.1.8.ª, 18.ª, 21.ª y 29.ª de la Constitución.

Disposición final segunda. *Desarrollo reglamentario.*

1. El Gobierno adaptará la regulación reglamentaria del documento nacional de identidad a las previsiones de esta ley.

2. Así mismo, se habilita al Gobierno para dictar las demás disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta ley.

Disposición final tercera. *Entrada en vigor.*

La presente ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

§ 12

Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

Ministerio del Interior
«BOE» núm. 307, de 24 de diciembre de 2005
Última modificación: 23 de noviembre de 2013
Referencia: BOE-A-2005-21163

La Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en su artículo 9, reconoce el derecho de todos los españoles a que se les expida el Documento Nacional de Identidad, al que se atribuye el valor suficiente para acreditar, por sí solo, la identidad de las personas y le otorga la protección que a los documentos públicos y oficiales es reconocida por el ordenamiento jurídico.

La misma norma dispone la obligatoriedad del Documento Nacional de Identidad para los mayores de catorce años, salvo en los supuestos en que, conforme a lo previsto en la Ley, haya de ser sustituido por otro documento, y establece también que en el mismo figurarán la fotografía y la firma del titular, así como los datos personales que se determinen reglamentariamente.

En cuanto a la competencia para su expedición y gestión, la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, atribuye al Cuerpo Nacional de Policía, la de la expedición del Documento Nacional de Identidad, al recogerla expresamente entre las funciones que encomienda a este Instituto Policial, el cual la misma Ley dispone que dependerá del Ministerio del Interior.

Por otra parte, la Ley 59/2003, de 19 de diciembre, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.

La misma Ley, en el apartado primero de la disposición final segunda dispone que el Gobierno adaptará la regulación reglamentaría del Documento Nacional de Identidad a las previsiones de la referida Ley.

Asimismo, ha de señalarse que la normativa reglamentaria que regula los distintos aspectos del Documento Nacional de Identidad se encuentra dispersa en distintas disposiciones y data, en parte, de fechas anteriores a la vigencia de la Constitución, lo que genera disfunciones a la hora de su aplicación, derivadas tanto de la propia antigüedad de las normas, como de la dispersión de estas.

En este contexto, y a la vista del mandato legal contenido en la Ley 59/2003, antes citada, resulta imprescindible acometer la adecuación y ordenación de la normativa que regula el referido Documento, abordando aquellos aspectos derivados de las nuevas utilidades que se le atribuyen.

En su virtud, a propuesta del Ministro del Interior, con la aprobación previa del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros, en su reunión del día 23 de diciembre de 2005,

D I S P O N G O :

Artículo 1. *Naturaleza y funciones.*

1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.

2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo.

3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.

4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.

5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

6. Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento.

Artículo 2. *Derecho y obligación de obtenerlo.*

1. Todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad, siendo obligatoria su obtención por los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.

2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo cuando fueren requeridas para ello por la Autoridad o sus Agentes.

Artículo 3. *Órgano competente para la expedición y gestión.*

1. Será competencia del Ministerio del Interior el ejercicio de las funciones relativas a la gestión, dirección, organización, desarrollo y administración de todos aquellos aspectos referentes a la expedición y confección del Documento Nacional de Identidad, conforme a lo previsto en la legislación en materia de seguridad ciudadana y de firma electrónica.

2. El ejercicio de las competencias a que se refiere el apartado anterior, incluida la emisión de los certificados de firma electrónica reconocidos, será realizado por la Dirección General de la Policía, a quien corresponderá también la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad. A tal efecto, la Dirección General de la Policía quedará sometida a las obligaciones impuestas al responsable del fichero por la Ley Orgánica 15/1999, de 13 de septiembre, de Protección de Datos de Carácter Personal.

Artículo 4. *Procedimiento de expedición.*

1. El Documento Nacional de Identidad se expedirá a solicitud del interesado en la forma y lugares que al efecto se determinen, para lo cual deberá aportar los documentos que se establecen en el artículo 5.1 de este Real Decreto.

2. En orden a facilitar a los ciudadanos la obtención del Documento Nacional de Identidad, el Ministerio del Interior en colaboración con el Ministerio de Administraciones Públicas adoptará las medidas oportunas para el fomento de la cooperación de los distintos órganos de las Administraciones Públicas con la Dirección General de la Policía.

Artículo 5. *Requisitos para la expedición.*

1. Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los siguientes documentos:

a) Certificación literal de nacimiento expedida por el Registro Civil correspondiente. A estos efectos únicamente serán admitidas las certificaciones expedidas con una antelación máxima de seis meses a la fecha de presentación de la solicitud de expedición del Documento Nacional de Identidad y que contengan la anotación de que se ha emitido a los solos efectos de la obtención de este documento.

b) Una fotografía reciente en color del rostro del solicitante, tamaño 32 por 26 milímetros, con fondo uniforme blanco y liso, tomada de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.

c) Certificado o volante de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del documento nacional de identidad.

d) Los españoles residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes.

2. Excepcionalmente, en los supuestos en que, por circunstancias ajenas al solicitante, no pudiera ser presentado alguno de los documentos a que se refiere el apartado primero de este artículo, y siempre que se acrediten por otros medios, suficientes a juicio del responsable del órgano encargado de la expedición, los datos que consten en tales documentos, se le podrá expedir un Documento Nacional de Identidad con la validez que se indica en el artículo siguiente.

3. En el momento de la solicitud, al interesado se le recogerán las impresiones dactilares de los dedos índices de ambas manos. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de ambos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden de prelación: medio, anular o pulgar; consignándose, en el lugar del soporte destinado a tal fin, el dedo utilizado, o la imposibilidad de obtener alguno de ellos.

Artículo 6. *Validez.*

1. Con carácter general el documento nacional de identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

a) Dos años cuando el solicitante no haya cumplido los cinco años de edad.

b) Cinco años, cuando el titular haya cumplido los cinco años de edad y no haya alcanzado los treinta al momento de la expedición o renovación.

c) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.

d) Permanente cuando el titular haya cumplido los setenta años.

2. De forma excepcional se podrá otorgar validez distinta al Documento Nacional de Identidad en los siguientes supuestos de expedición y renovación:

a) Permanente, a personas mayores de treinta años que acrediten la condición de gran inválido.

b) Por un año en los supuestos del apartado segundo del artículo 5 y del mismo apartado del artículo 7 siempre que, en éste último caso, no se puedan aportar los documentos justificativos que acrediten la variación de los datos.

3. No obstante lo dispuesto en este artículo, en cuanto a la validez de la utilidad informática prevista en el artículo 1.4 se estará a lo que específicamente se establece al respecto en el artículo 12 de este Real Decreto.

Artículo 7. *Renovación.*

1. Transcurrido el período de validez que para cada supuesto se contempla en el artículo anterior, el Documento Nacional de Identidad se considerará caducado y quedarán sin efecto las atribuciones y efectos que le reconoce el ordenamiento jurídico, estando su titular obligado a proceder a la renovación del mismo.

Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento, que deberá abonar la tasa correspondiente y aportar una fotografía con las características señaladas en el artículo 5.1.b). También se le recogerán las impresiones dactilares que se refieren en el apartado tercero del mismo artículo.

2. Independientemente de los supuestos del apartado anterior se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso aportar, además de lo establecido en el apartado anterior, los documentos justificativos que acrediten dicha variación.

Artículo 8. *Expedición de duplicados.*

1. El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación prevista en el apartado primero del artículo anterior. La validez de estos duplicados será la misma que tenían los Documentos a los que sustituyen, salvo que éstos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.

2. Los documentos sustituidos perderán el carácter de Documento Nacional de Identidad, así como los efectos que el ordenamiento jurídico atribuye a éste con respecto a su titular.

Artículo 9. *Entrega del Documento Nacional de Identidad.*

1. La entrega del documento nacional de identidad deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o sea una persona con capacidad judicialmente complementada, se llevará a cabo en presencia de quien tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas. En el momento de la entrega del documento nacional de identidad se proporcionará la información a que se refiere el artículo 18.b) de la Ley 59/2003, de 19 de diciembre.

2. La activación del certificado de firma electrónica en el documento nacional de identidad tendrá carácter voluntario y su utilización se realizará mediante una clave personal y secreta que el titular del documento nacional de identidad podrá introducir reservadamente en el sistema.

3. Al entregar el Documento renovado, se procederá a la retirada del anterior para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita.

Artículo 10. *Características de la tarjeta soporte.*

1. El material, formato y diseño de la tarjeta soporte del Documento Nacional de Identidad se determinará por el Ministerio del Interior, teniendo en cuenta en su elaboración la utilización de procedimientos y productos conducentes a la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación. Llevará incorporado un chip electrónico al objeto de posibilitar la utilidad informática a que se refiere el artículo 1.4 de este Real Decreto.

2. La tarjeta soporte llevará estampados en el anverso, de forma destacada y preeminente los literales «Documento Nacional de Identidad», «España» y «Ministerio del Interior».

Artículo 11. *Contenido.*

1. El Documento Nacional de Identidad recogerá gráficamente los siguientes datos de su titular:

En el anverso:

Apellidos y nombre.
Fecha de nacimiento.
Sexo.
Nacionalidad.
Número personal del Documento Nacional de Identidad y carácter de verificación correspondiente al Número de Identificación Fiscal.
Fotografía.
Firma.

En el reverso:

Lugar de nacimiento.
Provincia-Nación.
Nombre de los padres.
Domicilio.
Lugar de domicilio.
Provincia.
Nación.
Caracteres OCR-B de lectura mecánica.

Los datos de filiación se reflejarán en los mismos términos en que consten en la certificación a la que se alude en el artículo 5.1.a) de este Real Decreto, excepto en el campo de caracteres OCR-B de lectura mecánica, en que por aplicación de acuerdos o convenios internacionales la transcripción literal de aquellos datos impida o dificulte la lectura mecánica y finalidad de aquellos caracteres.

2. Igualmente constarán los siguientes datos referentes al propio Documento y a la tarjeta soporte:

Fecha de caducidad
Número de soporte.

3. Los textos fijos se expresarán en castellano y los expedidos en territorio de aquellas Comunidades Autónomas que tengan otra lengua oficial, serán también expresados en esta.

4. El chip incorporado a la tarjeta soporte contendrá:

Datos de filiación del titular.
Imagen digitalizada de la fotografía.
Imagen digitalizada de la firma manuscrita.
Plantilla de la impresión dactilar del dedo índice de la mano derecha o, en su caso, del que corresponda según lo indicado en el artículo 5.3 de este Real Decreto.
Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez.
Claves privadas necesarias para la activación de los certificados mencionados anteriormente.

Artículo 12. *Validez de los certificados electrónicos.*

1. Con independencia de lo que establece el artículo 6.1 sobre la validez del Documento Nacional de Identidad, los certificados electrónicos reconocidos incorporados al mismo tendrán un período de vigencia de treinta meses.

A la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente. Para la solicitud de un nuevo certificado deberá mediar la presencia física del titular en la forma y con los requisitos que se

determinen por el Ministerio del Interior, de acuerdo con lo previsto en la Ley 59/2003, de 19 de diciembre.

2. El cumplimiento del período establecido en el apartado anterior implicará la inclusión de los certificados en la lista de certificados revocados que será mantenida por la Dirección General de la Policía, bien directamente o a través de las entidades a las que encomiende su gestión.

3. La pérdida de validez del Documento Nacional de Identidad llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. La renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la expedición de nuevos certificados electrónicos.

4. También serán causas de extinción de la vigencia del certificado reconocido las establecidas en la Ley 59/2003, de 19 de diciembre, que resulten de aplicación, y, entre otras, el fallecimiento del titular del Documento Nacional de Identidad electrónico.

5. En los supuestos previstos en el artículo 8.1 de este Real Decreto, el titular deberá comunicar inmediatamente tales hechos a la Dirección General de la Policía por los procedimientos y medios que al efecto habilite la misma, al objeto de su revocación.

Artículo 13. *Declaración de Prácticas y Políticas de Certificación.*

De acuerdo y en cumplimiento del artículo 19 de la Ley 59/2003, de 19 de diciembre, el Ministerio del Interior formulará una Declaración de Prácticas y Políticas de Certificación. Dicha Declaración de Prácticas y Políticas de Certificación estará disponible al público de manera permanente y fácilmente accesible en la página de Internet del Ministerio del Interior.

Disposición adicional primera. *Documento de sustitución del Documento Nacional de Identidad en supuestos de retirada de éste.*

En los supuestos en que, de acuerdo con las previsiones establecidas en las Leyes, sea acordada por la Autoridad competente la retirada temporal de Documento Nacional de Identidad por los órganos encargados de la expedición de éste, se procederá a dotar al interesado de un documento identificador que tendrá las características y funcionalidades que determine el Ministerio del Interior, atendiendo a las causas de su retirada.

Disposición adicional segunda. *Documento Nacional de Identidad de los menores de edad.*

La posesión del Documento Nacional de Identidad por los menores de edad no supone, por sí sola, autorización para desplazarse fuera del territorio nacional, debiendo ser suplida, a estos efectos, con la correspondiente autorización de quien ejerza la patria potestad o tutela.

Disposición adicional tercera. *Imposibilidad de expedición o renovación del Documento Nacional de Identidad.*

Cuando exista imposibilidad manifiesta para la expedición del Documento Nacional de Identidad, y sin perjuicio de que por las Autoridades y Órganos correspondientes se compruebe la personalidad del interesado por cualesquiera otros medios, excepcionalmente podrá sustituirse aquél por certificaciones anuales en las que consten los motivos de tal imposibilidad, que en los supuestos de renovación tendrán únicamente el fin de prorrogar la validez del Documento caducado.

Disposición adicional cuarta. *Remisión de información por vía telemática.*

1. La documentación requerida para la expedición del Documento Nacional de Identidad en el artículo 5.1 de este Real Decreto no será exigible cuando sea posible remitir ésta desde los órganos competentes por medios telemáticos a la Dirección General de la Policía, de conformidad con lo que se establezca mediante Convenio.

2. En estos casos, por Orden del Ministro del Interior se establecerá el régimen de aportación de dichos documentos.

Disposición transitoria única. *Validez de los Documentos Nacionales de Identidad expedidos o renovados de conformidad con la normativa anterior a este Real Decreto y proceso de sustitución.*

1. Los Documentos Nacionales de Identidad ya emitidos o los que se continúen expidiendo por el sistema anterior conforme a la normativa existente a la entrada en vigor de este Real Decreto seguirán siendo válidos y eficaces de conformidad con dicha normativa en tanto no se proceda a su sustitución por el Documento Nacional de Identidad de acuerdo con lo que se establece en el apartado siguiente de esta disposición.

2. La Dirección General de la Policía programará y organizará, temporal y territorialmente el proceso de sustitución de las tarjetas soporte del Documento Nacional de Identidad emitidas con anterioridad a la entrada en vigor de este Real Decreto por el nuevo Documento Nacional de Identidad, pudiendo establecerse por razones de interés público programaciones especiales para determinados colectivos.

3. Sólo se podrá solicitar la expedición del nuevo Documento Nacional de Identidad en el marco de la programación a que se hace referencia en el apartado anterior.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas las siguientes disposiciones: Decreto 196/1976, de 6 de febrero, por el que se regula el Documento Nacional de Identidad, y las modificaciones llevadas a cabo en el mismo a través de los Reales Decretos 1189/1978, de 2 de junio; 2002/1979, de 20 de julio; 2091/1982, de 12 de agosto; y 1245/1985, de 17 de julio.

2. Asimismo, quedan derogadas todas aquellas normas de igual o inferior rango que se opongan a lo preceptuado en este Real Decreto.

Disposición final primera. *Título competencial.*

Este Real Decreto se dicta al amparo de las competencias atribuidas al Estado por el artículo 149.1.8.ª,18.ª, 21.ª y 29.ª de la Constitución.

Disposición final segunda. *Desarrollo.*

1. El Ministerio del Interior adoptará las disposiciones necesarias para dar cumplimiento a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, en materia de creación y modificación de ficheros de titularidad pública.

2. Se habilita a los Ministros del Interior, de Justicia, de Economía y Hacienda, de Industria, Turismo y Comercio y de Administraciones Públicas para que dicten, en el ámbito de sus respectivas competencias, cuantas disposiciones sean necesarias para el desarrollo y aplicación de este Real Decreto.

Disposición final tercera. *Tasas.*

El Gobierno promoverá la norma legal de rango adecuado para la adecuación de la tasa que haya de percibirse por la expedición del Documento Nacional de Identidad, de acuerdo con su coste y en consideración a los beneficios que proporciona a la comunidad.

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», excepto lo relativo al artículo 1.4 que entrará en vigor cuando lo haga el nuevo formato y diseño del Documento Nacional de Identidad.

§ 13

Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre

Ministerio de la Presidencia
«BOE» núm. 88, de 12 de abril de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-5788

Una de las manifestaciones más relevantes de la Administración electrónica es la práctica de notificaciones por medios electrónicos, informáticos y telemáticos por las distintas Administraciones Públicas. Esta posibilidad, vislumbrada en el artículo 70 de la Ley 30/1992, cobró carta de naturaleza específica cuando la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, incorporo sendos textos de idéntico tenor en los artículos 105 de la Ley General Tributaria y 59 de la Ley 30/1992, configurando un nuevo modelo de notificación mediante la puesta a disposición de la actuación correspondiente de manera que los efectos de la notificación se producen bien por el acceso a su contenido bien por el simple transcurso del lapso de diez días desde la puesta a disposición sin que tenga lugar dicho acceso por parte del destinatario. El Real Decreto 209/2003, de 21 de febrero, desarrolla esta última previsión, siendo su disposición final primera desarrollada a su vez por la Orden PRE/1551/2003, de 10 de junio, con el objeto de establecer los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse y las condiciones que han de reunir el órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única así como las condiciones de su prestación. Toda la regulación de la notificación electrónica se fundamenta en la existencia de una única dirección electrónica a tal efecto en el ámbito de la Administración del Estado y en su carácter voluntario.

La Ley 11/2007, de 11 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, regula de modo similar la notificación por medios electrónicos, admitiendo que en determinados supuestos pueda establecerse esta notificación con carácter obligatorio. El reciente Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, desarrolla en su artículo 38 la notificación mediante la puesta a disposición del documento electrónico a través de dirección electrónica habilitada, previendo que bajo responsabilidad del Ministerio de la Presidencia existirá un sistema de dirección electrónica habilitada para la práctica de estas notificaciones que quedará a disposición de todos los órganos y organismos públicos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios. Además, en su apartado segundo se establece que «Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada a que se refiere el apartado anterior será asignada de oficio y podrá tener vigencia indefinida, conforme al régimen que

se establezca por la orden del Ministro de la Presidencia a la que se refiere la disposición final primera».

En su virtud, previo informe del Consejo Superior de Administración Electrónica, dispongo:

Artículo 1. *Objeto.*

La presente Orden tiene por objeto establecer el régimen de un sistema de notificación mediante dirección electrónica habilitada, a disposición de los órganos y organismos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios, tanto en los casos de notificación voluntaria como cuando tenga carácter obligatorio, de acuerdo con lo previsto en el artículo 38 y en la disposición final primera del Real Decreto 1671/2009, de 8 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.

Artículo 2. *Dirección electrónica habilitada responsabilidad del Ministerio de la Presidencia.*

1. La titularidad de la dirección electrónica a partir de la cual se construyan las direcciones electrónicas habilitadas de los interesados, corresponde al Ministerio de la Presidencia.

2. La prestación del servicio de dirección electrónica habilitada se llevará a cabo por el Ministerio de la Presidencia, directamente, o a través del prestador que se establezca conforme a lo dispuesto en el ordenamiento jurídico.

3. El directorio del servicio de dirección electrónica habilitada deberá recoger el nombre y apellidos o la razón o denominación social del interesado, el número de identificación fiscal y la dirección electrónica habilitada.

4. El sistema de dirección electrónica habilitada se sujetará a lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como a la normativa protectora en materia de datos de carácter personal.

Artículo 3. *Asignación de dirección electrónica habilitada.*

1. Se asignará una dirección electrónica habilitada, con la inclusión en el correspondiente directorio, cuando el interesado solicite su apertura.

2. Asimismo se asignará en todo caso de oficio una dirección electrónica cuando se reciba de un órgano u organismo de la Administración General del Estado el aviso para la práctica de una notificación conforme al sistema establecido en la presente Orden.

Artículo 4. *Vigencia.*

1. La dirección electrónica habilitada tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará esta dirección electrónica, comunicándose así al interesado.

2. No obstante, no se inhabilitará esta dirección electrónica cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, y así se confirme por los órganos u organismos afectados al prestador del servicio de dirección electrónica.

Artículo 5. *Autenticación.*

1. La identificación y autenticación de la notificación se hará por alguno de los medios admitidos conforme a la ley 11/2007 y de acuerdo con lo establecido por el Real Decreto 1671/2009.

2. La autenticación de los ciudadanos en el acceso al contenido del documento notificado se hará mediante certificados electrónicos que se admitan conforme a lo establecido en la normativa vigente.

3. En particular, las personas jurídicas y entidades sin personalidad podrán acceder al contenido del documento notificado mediante los certificados electrónicos que se admitan.

Artículo 6. *Confidencialidad.*

1. El sistema de notificación electrónica contendrá mecanismos de cifrado para proteger la confidencialidad de los datos en las transmisiones.

2. Asimismo, el sistema contará con las medidas de seguridad adecuadas para que el prestador del servicio de dirección electrónica habilitada no acceda al contenido de los actos y actuaciones administrativas que se notifiquen.

Artículo 7. *Referencia temporal.*

1. El sistema de notificación electrónica acreditará las fechas y horas en que se produzca la puesta a disposición del interesado del acto objeto de notificación. Ello tendrá lugar mediante la recepción en la dirección electrónica asignada al destinatario del aviso de la puesta a disposición de la notificación, incluyendo el propio documento que se notifica o, al menos, su huella electrónica.

Para la referencia temporal de los actos y certificaciones se utilizará una marca de tiempo entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora. La fecha y hora utilizada se sincronizará 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 el 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 según las condiciones técnicas y protocolos que el citado Organismo establezca.

La información relativa a las marcas de tiempo se asociará en la forma que determine el Esquema Nacional de Interoperabilidad.

2. El sistema de dirección electrónica habilitada acreditará igualmente el acceso del destinatario al contenido del documento notificado, así como cualquier causa técnica que imposibilite alguna de las circunstancias de este artículo.

Artículo 8. *Seguridad.*

1. Los órganos de la Administración General del Estado y los organismos públicos vinculados o dependientes de aquélla que pongan en marcha dispositivos y aplicaciones de registro y notificación deben adoptar medidas de seguridad para la salvaguarda de la confidencialidad. En cualquier caso establecerán las siguientes medidas:

a) Medidas de seguridad física.

b) Control de los accesos a los dispositivos y aplicaciones de registro y notificación, en especial los que lleguen a través de las redes de comunicaciones.

c) Protección de los soportes de información y copias de respaldo.

d) Cifrado de las notificaciones, cuando así se establezca por la legislación sobre protección de los datos de carácter personal o lo estime necesario el órgano u organismo notificador.

2. El prestador del servicio de dirección electrónica única designará a un responsable de la seguridad, que se encargará de la realización y actualización del análisis y gestión de riesgos, del registro de incidencias de seguridad, de la correcta implementación de las salvaguardas de seguridad técnicas, organizativas, y de cuantas otras actuaciones en materia de seguridad sean necesarias para la protección de los sistemas a su cargo.

Artículo 9. *Disponibilidad.*

1. El sistema de dirección electrónica habilitada posibilitará el acceso permanente de los interesados a la dirección electrónica correspondiente, tanto para solicitar la asignación de una dirección electrónica habilitada como para acceder al contenido de las notificaciones puestas a su disposición.

2. El acceso se producirá a través del Punto de Acceso General de la Administración General del Estado, así como de las sedes electrónicas del Ministerio de la Presidencia y de

los órganos u organismos adheridos al sistema o, en su caso, del prestador del servicio de dirección electrónica.

3. Los órganos y organismos a los que se refiere el artículo anterior adoptarán las medidas organizativas y técnicas para garantizar la disponibilidad del servicio 7 días a la semana y 24 horas al día, y en cualquier caso las siguientes:

a) Adopción de medidas de protección frente a código dañino en los servidores de aplicación y en los soportes circulantes.

b) Preparación y mantenimiento operativo de un plan de contingencia.

Artículo 10. *Condiciones de prestación del servicio.*

1. El órgano, organismo o entidad al que, en su caso, corresponda la prestación del sistema de dirección electrónica habilitada, llevará a cabo las siguientes funciones:

a) Crear y mantener el directorio de direcciones electrónica habilitadas con la información proporcionada por los interesados.

b) Almacenar y custodiar los avisos de puesta a disposición en la dirección electrónica habilitada.

c) Gestionar los acuses de recibo de los interesados y de los órganos u organismos notificadores.

d) Mantener el registro de eventos de las notificaciones, el cual contendrá, al menos, la dirección electrónica, la traza de la fecha y la hora de la recepción de la puesta a disposición en la dirección electrónica y del acceso del interesado a la notificación y la descripción del contenido de la notificación.

e) Impedir el acceso al contenido de las notificaciones que se entienden rechazadas por el transcurso de diez días desde su puesta a disposición.

f) Establecer las medidas organizativas y técnicas para que la disponibilidad del servicio sea de siete días a la semana y veinticuatro horas al día.

g) Potestativamente, otras funciones de mejora del servicio y complementarias de las expresadas, como es el caso de aviso de puesta a disposición de los interesados de las notificaciones mediante mensajería o de cualquier otro modo.

2. El prestador del servicio de dirección electrónica habilitada deberá remitir al órgano u organismo actuante por cada notificación electrónica:

a) Certificación electrónica de la fecha y hora en la que recibe el aviso de puesta a disposición enviada por el órgano u organismo notificador.

b) Certificación electrónica de la fecha y hora en la que se produce la recepción en la dirección electrónica asignada al destinatario del aviso de la puesta a disposición de la notificación, incluyendo el propio acto o actuación notificada o, al menos, su sello electrónico.

c) Certificación electrónica en la que conste la fecha y hora en la que se produce el acceso del interesado al contenido de la notificación en la dirección electrónica.

d) Certificación electrónica del transcurso del plazo de diez días desde la puesta a disposición sin que se haya producido el acceso del interesado al contenido de la notificación en la dirección electrónica.

e) Certificación electrónica de cualquier incidencia que se produzca en la práctica de lo dispuesto en los apartados anteriores.

3. En el caso de cese de actividad o cambio del prestador del servicio de dirección electrónica, las bases de datos, los programas informáticos asociados, el registro de eventos y el dominio de direcciones electrónicas con las notificaciones que existan en ese momento y la documentación técnica, deberán entregarse al Ministerio de la Presidencia, o a la entidad que éste designe debidamente actualizadas.

4. Los programas necesarios para el correcto funcionamiento del sistema de notificación serán suministrados a los órganos y organismos notificadores por el prestador del servicio de dirección electrónica habilitada.

Disposición transitoria única. *Mantenimiento de la prestación del servicio.*

1. A la entrada en vigor de la presente Orden, la prestación del servicio de dirección habilitada seguirá realizándose a través de los servicios autorizados, de conformidad con la Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por la que se regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

2. En el plazo de tres meses desde la entrada en vigor de la presente Orden se llevarán a cabo las adaptaciones requeridas en la prestación del servicio de dirección habilitada.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en esta Orden, y, especialmente, la Orden PRE/1551/2003, de 10 de junio, que desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, que regula los registros y notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de certificados por los ciudadanos.

Disposición final. *Entrada en vigor.*

La presente orden entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 5 de abril de 2010.La Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, María Teresa Fernández de la Vega Sanz.

§ 14

Orden EHA/1307/2005, de 29 de abril, por la que se regula el empleo de medios electrónicos en los procedimientos de contratación

Ministerio de Economía y Hacienda
«BOE» núm. 114, de 13 de mayo de 2005
Última modificación: sin modificaciones
Referencia: BOE-A-2005-7774

La implantación de un efectivo y fiable sistema de administración electrónica que se extienda a todas las esferas de la actividad administrativa constituye uno de los principales retos que ha de afrontar la Administración de cara a definir un nuevo sistema, más eficaz y transparente, de relaciones con los ciudadanos.

Ya la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, promulgada en un momento en que las tecnologías de la información y de la comunicación comenzaban un desarrollo que se aceleraría en el transcurso de la década, anticipó la necesidad de insertar plenamente estos nuevos instrumentos en la actividad administrativa instando, desde su artículo 45, a las Administraciones Públicas para que promuevan la incorporación de técnicas electrónicas, informáticas y telemáticas en el desarrollo de su actividad y en el ejercicio de sus competencias. En igual sentido, la reforma de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común efectuada por la Ley 24/2001, de 27 de diciembre, de medidas Fiscales, Administrativas y del Orden Social, tuvo por finalidad potenciar el uso de medios electrónicos, informáticos y telemáticos por la Administración.

Las previsiones de la Ley 30/1992 fueron desarrolladas por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias y documentos y devolución de originales y el régimen de las oficinas de registro, ambos modificados por el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, normas que, en conjunción con sus antecedentes legales, constituyen la base general para el uso de medios electrónicos en el ámbito administrativo.

Sobre este base general, la presente Orden viene a regular, al amparo de la disposición adicional décima del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto 1098/2001, de 12 de octubre, las especialidades del uso de los medios electrónicos en el procedimiento de contratación, cuya particular consideración frente al resto de procedimientos administrativos, por razón de su peculiar naturaleza, viene reconocida por la disposición adicional séptima del texto refundido de la

Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio. En la redacción de la Orden, por otra parte, se han tenido particularmente en cuenta las directrices de la Directiva 2004/18/CE, del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios, de la que constituyen una parte esencial las provisiones dirigidas a introducir sistemas efectivos de licitación electrónica en la contratación pública europea.

Desde un punto de vista práctico, la contratación administrativa es un ámbito en el que la correcta implantación de medios electrónicos puede producir especiales beneficios, para la Administración y para los operadores económicos, generando importantes ahorros de tiempo y costes y contribuyendo decisivamente a incrementar el nivel de competencia, transparencia y control. Por ello, se considera urgente incorporar las tendencias antes apuntadas sobre tramitación telemática de los expedientes administrativos al ámbito de la contratación, sentando las bases normativas que posibiliten la articulación, a corto plazo, de sistemas electrónicos en esta área de actividad; ello permitirá generar la necesaria experiencia en la aplicación de las nuevas tecnologías de la información y de la comunicación a los procedimientos legales de contratación que, eventualmente, podría servir de base a una revisión más profunda de su configuración, todo ello sin renunciar a la deseable homologación de soluciones cuando se desarrollen y adopten de forma mayoritaria estándares europeos para la contratación electrónica.

Ha de señalarse, por último, que a pesar del carácter de norma básica que tiene la disposición adicional décima del Reglamento General de la Ley de Contratos de las Administraciones Públicas, base jurídica de la presente Orden, ésta limita su eficacia al ámbito estatal, por estimarse preferible esperar a que se decanten suficientemente las medidas de implementación del marco normativo constituido por la Directiva 2004/18/CE que, impulsadas desde instancias comunitarias, se dirigen a estandarizar los sistemas y aplicaciones utilizados en la licitación electrónica para garantizar su interoperabilidad y el intercambio de datos entre las Administraciones europeas, y a que se consolide suficientemente una experiencia en el empleo de estos medios que permita identificar con mayor seguridad aquellos extremos de la contratación electrónica cuya homogeneidad deba garantizarse mediante su regulación por disposiciones de carácter básico.

En su virtud, previo informe de la Junta Consultiva de Contratación Administrativa y con la aprobación del Ministro de Administraciones Públicas, dispongo:

Primero. *Objeto y ámbito de aplicación.*

La presente Orden tiene por objeto regular, al amparo de lo dispuesto en la disposición adicional décima del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto 1098/2001, de 12 de octubre, la utilización de medios electrónicos en los procedimientos de contratación sujetos a las prescripciones del texto refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio, que se tramiten por la Administración General del Estado, sus Organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social y demás entidades públicas estatales, así como por las sociedades de derecho privado vinculadas a las anteriores.

Segundo. *Condiciones para el empleo de medios electrónicos en los procedimientos de contratación.*

Uno. Podrán utilizarse medios electrónicos en los procedimientos de contratación siempre que en los pliegos de cláusulas administrativas particulares se haya establecido su admisibilidad. A estos efectos, los pliegos deberán indicar los trámites que, en su caso, puedan ser cumplimentados por vía electrónica, informática o telemática, y los medios electrónicos y sistemas de comunicación y notificación utilizables, que deberán ajustarse a las especificaciones detalladas en el apartado tercero de esta Orden.

En estos supuestos, los pliegos y la restante documentación necesaria para tomar parte en la licitación deben estar disponibles para los interesados en forma electrónica, en un formato conforme con los estándares abiertos aplicables a cada documento, y ser accesibles a través de procedimientos electrónicos de carácter no discriminatorio, de acceso público, y

compatibles con las tecnologías de la información y de la comunicación de uso general. En el caso de que el medio de difusión elegido sea Internet el formato de dichos documentos deberá ser conforme con las Recomendaciones aplicables aprobadas por el World Wide Web Consortium (W3C).

Dos. Cuando, conforme a lo señalado en el punto anterior, los pliegos hayan admitido el empleo de medios electrónicos, informáticos o telemáticos en el procedimiento de contratación, su uso será potestativo para los licitadores.

El licitador que desee utilizar estos medios en sus relaciones con el órgano de contratación deberá presentar por vía electrónica su proposición o solicitud de participación y la documentación que, según el pliego, pueda remitirse en esta forma y manifestar expresamente, al mismo tiempo, que opta por el empleo de medios electrónicos para la presentación de escritos, comunicaciones y documentos y para la recepción de notificaciones, a cuyo efecto debe estar dado de alta en un sistema de notificación telemática admitido por el órgano de contratación en el pliego y disponer de una dirección electrónica, con los requisitos indicados en el numero cinco del apartado tercero de esta Orden.

La opción por el uso de medios electrónicos vincula al licitador durante toda la fase de licitación del contrato y, si llegara a ser el adjudicatario del mismo, durante el período de su ejecución, constituyéndole en la obligación de utilizar los programas, formatos y aplicaciones establecidos, salvo que causas técnicas, debidamente acreditadas, lo impidan.

En ningún caso podrá derivarse para los licitadores y contratistas una discriminación o restricción de cualquier naturaleza contraria a los principios de libre concurrencia e igualdad de trato por razón de los medios por los que opten para efectuar sus comunicaciones con el órgano de contratación.

Tres. No obstante lo señalado en el número anterior, en los contratos en que, por razón del número previsible de licitadores, por la cantidad y características de los productos o bienes objeto de licitación, o por la concurrencia de otras peculiaridades debidamente motivadas, se considere conveniente por razones de agilidad y simplificación del procedimiento y, en todo caso, en las licitaciones y contratos que se celebren dentro del sistema de adquisición centralizada de bienes y servicios al amparo de los artículos 183 y 199 de la Ley de Contratos de las Administraciones Públicas, los pliegos de cláusulas administrativas podrán establecer la necesidad de que la presentación de las solicitudes de participación y proposiciones, la aportación de documentos y las comunicaciones y notificaciones entre el órgano de contratación y los licitadores o contratistas, se realicen, en todas o en alguna de sus fases, de forma exclusiva, por medios electrónicos.

Para que en los pliegos pueda establecerse la necesaria utilización de medios electrónicos, deberá acreditarse en el expediente de contratación, que esta exigencia no supondrá restricción o discriminación alguna para los licitadores, en el sentido señalado en la disposición adicional decimoctava de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Tercero. *Requisitos y especificaciones técnicas de los medios electrónicos utilizables en la contratación administrativa.*

Uno. Con carácter general se aplicarán a los dispositivos y aplicaciones de registro, notificación y de la prestación del servicio de dirección electrónica las medidas de seguridad, conservación y normalización que se detallan en los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» aprobados por el Consejo Superior de Informática y para el impulso de la Administración Electrónica y accesibles en su sitio web.

Dichas medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la metodología Magerit.

Dos. Los sistemas de comunicaciones y para el intercambio y almacenamiento de información deberán garantizar la integridad de los datos y la confidencialidad de las ofertas y solicitudes de participación.

Los medios electrónicos utilizables en los procedimientos de contratación no podrán ser discriminatorios, y deberán ser de acceso público y compatibles con las tecnologías de la

información y de la comunicación de uso general, de forma que no se restrinja indebidamente el acceso de los operadores económicos al procedimiento de adjudicación.

Tres. La información, las especificaciones técnicas, y los programas y aplicaciones necesarios para la presentación electrónica de las ofertas y solicitudes de participación deberán estar a disposición de todas las partes interesadas.

Cuatro. Los formatos que el órgano de contratación declare admisibles en los pliegos para la aportación de documentos electrónicos deberán ser conformes a los estándares abiertos que se especifican en el anexo de esta norma.

Cinco. Los medios electrónicos que se utilicen en el procedimiento de contratación deben poder garantizar, de forma razonable en función del estado de la técnica, el cumplimiento de los siguientes requerimientos:

a) Que la firma electrónica reconocida exigida por el número dos del apartado cuarto de esta Orden se ajusta a las disposiciones de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

b) Que sólo los órganos competentes, en la fecha señalada para ello, pueden tener acceso a los datos transmitidos o que en caso de violación de la prohibición de acceso, esta violación pueda detectarse con claridad.

c) Que se deje un rastro de auditoría que permita el control posterior de las transacciones efectuadas.

Seis. El sistema de notificación telemática que se utilice deberá acreditar la fecha y hora en que se produzcan la recepción de la notificación en la dirección electrónica asignada al interesado y el acceso de éste al contenido del mensaje, así como poner de manifiesto cualquier incidencia técnica que imposibilite el cumplimiento de lo anterior. Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran diez días naturales sin que se acceda a su contenido se entenderá que la notificación ha sido rechazada.

La dirección electrónica asignada al licitador deberá cumplir los siguientes requisitos:

a) Poseer identificadores de usuario y claves de acceso para garantizar la exclusividad de su uso,

b) contar con mecanismos de autenticación que garanticen la identidad del usuario, y

c) contar con mecanismos para proteger la confidencialidad de los datos.

Siete. Atendiendo al grado de desarrollo y consolidación de los trabajos de normalización internacional, los documentos electrónicos que se utilicen en el procedimiento de contratación deberán adaptarse a la nomenclatura y estándares adoptados en el seno del programa para la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y ciudadanos (programa IDA/IDABC) en relación con las compras electrónicas o en su caso a otros estándares internacionales de carácter abierto.

Cuarto. *Régimen de las comunicaciones y notificaciones telemáticas.*

Uno. En todo lo no previsto en esta Orden, la validez y los efectos jurídicos de las comunicaciones y de las notificaciones telemáticas se regirán por lo establecido 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, en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y en el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias y documentos y devolución de originales y el régimen de las oficinas de registro, modificado por el Real Decreto 209/2003, de 21 de febrero.

Dos. Todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos y se emitan tanto en la fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato deben ser autenticados mediante una firma electrónica reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Tres. Las aplicaciones que se utilicen para efectuar las comunicaciones, notificaciones y envíos documentales entre el licitador o contratista y el órgano de contratación deben permitir acreditar la fecha y hora de su emisión o recepción, su contenido y el remitente y destinatario de las mismas. En especial, estas aplicaciones deben garantizar que se deja constancia de la hora y la fecha exactas de la recepción de las proposiciones o solicitudes de participación y de cuanta documentación deba presentarse ante el órgano de contratación.

Cuatro. En los documentos, comunicaciones y notificaciones telemáticas deberá usarse el juego de caracte-res ISO/IEC-8859-1 («latin alphabet -1»).

Cinco. Las proposiciones o solicitudes de participación, así como la documentación que se presente se enviarán libres de virus informáticos que dificulten o imposibiliten su lectura, siendo responsabilidad de los licitadores velar por el cumplimiento de esta previsión. No obstante, la mera presencia de virus en tales documentos no determinará, por sí sola, su exclusión de la licitación siempre que sea posible acceder a su contenido esencial y que resulte indubitable que los términos de la oferta no han sido alterados por efecto del virus.

Quinto. *Transmisión electrónica de datos entre órganos administrativos.*

Uno. Los órganos de contratación podrán recabar los datos y los documentos referentes a la empresa que, de conformidad con lo establecido en el artículo 79 de la Ley de Contratos de las Administraciones Públicas, requiera el pliego de cláusulas administrativas, especialmente los correspondientes a su capacidad y solvencia, de los órganos y registros de las Administraciones y Entidades públicas mediante interconexión electrónica con sus bases de datos y documentales, si el licitador o su representante así lo solicitan, indicando el lugar en que dichos datos y documentos consten o se encuentren, y siempre que, con arreglo a las normas vigentes, sea posible reconocer eficacia jurídica a los mismos, con respeto, en todo caso, a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Dos. Los registros de licitadores de la Administración General del Estado, sus Organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social y demás entidades públicas estatales facilitarán por medios electrónicos a los órganos y a las mesas de contratación dependientes de cualquiera de ellas que así lo requieran, certificaciones sobre la personalidad, capacidad de obrar y representación de las empresas inscritas, en la forma y con los efectos previstos en la Orden HAC/664/2004, de 9 de marzo, por la que se establecen los mecanismos de coordinación entre los registros voluntarios de licitadores.

Asimismo, con la autorización de las empresas inscritas y mediante el oportuno convenio de colaboración basado en el principio de reciprocidad, estos certificados electrónicos podrán ser facilitados a otras Administraciones Públicas, a los efectos de la participación de las empresas en sus propios procedimientos de contratación.

Sexto. *Apertura de proposiciones.*

Uno. En los casos en que el órgano de contratación establezca en los pliegos la necesidad de que las proposiciones se presenten cifradas, una vez realizadas las actuaciones previstas en los artículos 81 y 82 del Reglamento General de la Ley de Contratos de las Administraciones Públicas y en el acto público a que se refiere el artículo 83, deberá procederse, en primer término, a descifrar los ficheros que contengan la documentación correspondiente.

Dos. En el caso de que no pueda descifrarse alguno de los ficheros presentados, se rechazará la proposición si ello fuese debido a una causa imputable al licitador. Si por causas no imputables al licitador, surgieran circunstancias que impidieran el desciframiento, se suspenderá el acto hasta que por la mesa de contratación pueda subsanarse la incidencia de conformidad con lo previsto en el Reglamento General de la Ley de Contratos de las Administraciones Públicas, en cuyo momento se reanudará el mismo.

Séptimo. *Coordinación de los sistemas.*

Los sistemas de notificación y registro a los que se refiere la presente orden se coordinarán adecuadamente con los que, en su caso, se creen al amparo de lo dispuesto en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado y en el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, modificado por el Real Decreto 209/2003, de 21 de febrero.

Octavo. *Instrucciones.*

El Director General del Patrimonio del Estado dictará las instrucciones que resulten precisas para facilitar la adaptación a los estándares y nomenclatura a los que se refiere el número siete del apartado tercero de la presente orden, que garanticen la compatibilidad e interoperabilidad de los sistemas de información y comunicación que intervienen en los procesos de contratación electrónica, pudiendo, a estos efectos, modificar el anexo de esta Orden con el fin de incluir nuevos formatos que cumplan con los requisitos exigidos.

Noveno. *Regulación del uso de medios electrónicos en los procedimientos de contratación centralizada de bienes y servicios.*

En los procedimientos de contratación centralizada de bienes y servicios, las condiciones de uso de medios electrónicos podrán regularse, con arreglo a lo establecido en esta Orden, además de en los pliegos de cláusulas administrativas particulares, por resolución del Director General del Patrimonio del Estado.

Décimo. *Modificación del Anexo VII del Reglamento General de la Ley de Contratos de las Administraciones Públicas.*

Haciendo uso de la habilitación conferida por la disposición adicional sexta del Reglamento General de la Ley de Contratos de las Administraciones Públicas, se modifican los modelos de anuncios del anexo VII del dicho Reglamento que a continuación se indican, en el siguiente sentido:

En el modelo B), «Modelo de anuncio para la licitación de los contratos de obras», se añadirá un apartado con la siguiente redacción:

«14. En su caso, sistema de notificación telemática aplicable.»

En el modelo C), «Modelo de anuncio para la licitación de los contratos de gestión de servicios públicos», se añadirá un apartado con la siguiente redacción:

«13. En su caso, sistema de notificación telemática aplicable.»

En el modelo D), «Modelo de anuncio para la licitación de los contratos de suministro», se añadirá un apartado con la siguiente redacción:

«14. En su caso, sistema de notificación telemática aplicable.»

En el modelo E), «Modelo de anuncio para la licitación de los contratos de consultoría y asistencia y de servicios», se añadirá un apartado con la siguiente redacción:

«14. En su caso, sistema de notificación telemática aplicable.»

En el modelo F), «Modelo de anuncio para la licitación de los contratos administrativos especiales», se añadirá un apartado con la siguiente redacción:

«13. En su caso, sistema de notificación telemática aplicable.»

Undécimo. *Entrada en vigor.*

Uno. La presente Orden entrará en vigor a los dos meses de su publicación en el Boletín Oficial del Estado salvo lo dispuesto en el apartado noveno que entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

Dos. No obstante, durante un plazo de dos años a partir de la entrada en vigor de la presente Orden, los órganos de contratación podrán seguir empleando los formatos para el intercambio de datos que estén usando, siempre que respondan a estándares comúnmente aceptados y que su uso no sea contrario a los principios de libertad de acceso y no discriminación.

ANEXO

Formatos admisibles para los documentos intercambia-dos en los procesos de contratación electrónica

1. Formatos de datos estructurados.

1.1 Formato de documentos de datos: XML.
Estándar aplicable: XML 1.1 (Recomendación del W3C, 4 de febrero de 2004).
1.2 Formato de documentos de validación: XML Schema Language.
Estándar aplicable: XML Schema Language 1.1 (Recomendación del W3C, 2 de mayo de 2001).

2. Formato de documentos de texto y documentos compuestos: ISO-HTML.
Estándar aplicable: ISO/IEC 15445.

3. Formatos de gráficos e imágenes:

a) Formato: JPEG.
Estándar aplicable: ISO/IEC 10918.
b) Formato: TIFF.
Estándar aplicable: ISO/IEC 12234.
c) Formato: PNG.
Estándar aplicable: ISO/IEC 15948.
d) Formato: CGM.
Estándar aplicable: ISO/IEC 12071.

§ 15

Orden EHA/1220/2008, de 30 de abril, por la que se aprueban las instrucciones para operar en la Plataforma de Contratación del Estado

Ministerio de Economía y Hacienda
«BOE» núm. 105, de 1 de mayo de 2008
Última modificación: sin modificaciones
Referencia: BOE-A-2008-7708

La Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, con el fin de fomentar la transparencia de la actividad contractual del sector público, regula el Perfil de Contratante como medio preferente de difusión de tal información, basado en el Perfil de Comprador previsto en la Directiva 2004/18/CE, de 31 de marzo de 2004, sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios. Así, el artículo 42 de la Ley 30/2007 prevé que los órganos de contratación harán accesible a través de Internet su Perfil de Contratante, el cual podrá incluir cualesquiera datos e informaciones referentes a la actividad contractual del órgano de contratación, además de los aspectos que la Ley de Contratos del Sector Público establece como de necesaria publicación.

El artículo 309 de la Ley 30/2007 señala que la Junta Consultiva de Contratación Administrativa del Estado pondrá a disposición de todos los órganos de contratación del sector público una plataforma electrónica que permita dar publicidad a las convocatorias de licitaciones, a sus resultados y al resto de información contractual considerada relevante. La Plataforma de Contratación del Estado sirve así de espacio virtual de contacto entre los órganos de contratación del sector público y los interesados, pudiendo estos últimos acceder a la misma a través de un portal único.

En la Plataforma de Contratación del Estado se publicarán necesariamente los perfiles de contratante de los órganos de contratación de la Administración General del Estado, sus Organismos autónomos, Entidades gestoras y Servicios Comunes de la Seguridad Social y demás Entidades públicas estatales. Voluntariamente, además, se publicarán en esta Plataforma los perfiles de contratante de los restantes entes del sector público estatal y de los órganos de contratación de las Comunidades Autónomas y las Entidades Locales.

Además de la publicación voluntaria de los perfiles de contratante de los órganos de contratación de las Comunidades Autónomas y de las Entidades locales, la Plataforma de Contratación del Estado se interconectará con los servicios de información similares que articulen esas Administraciones Territoriales en la forma que determinen los convenios que se concluyan al efecto.

Para la operatividad de la Plataforma, resulta necesario establecer las directrices para que los órganos de contratación y demás órganos con competencias en materia de contratos públicos puedan proceder a publicar la información relevante a través de la Plataforma, así como definir las especificaciones CODICE que se utilizarán en la Plataforma. Todo ello sin

perjuicio que éstos documentos no puedan ser utilizados en la tramitación de expedientes de gasto a efectos de fiscalización previa, hasta que no se produzca la correspondiente adaptación de los sistemas orientados al control prevista para el 1 de junio de 2008.

En virtud de lo anterior, en ejercicio de las competencias atribuidas por el apartado 2 de la disposición final novena de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, dispongo:

CAPÍTULO I

Disposiciones Generales

Artículo 1. *Puesta en funcionamiento y dirección en INTERNET.*

La Plataforma de Contratación del Estado estará operativa a partir del día 2 de mayo de 2008, siendo accesible en la dirección http://www.contrataciondelestado.es,

En la Plataforma podrán publicar su Perfil de Contratante los órganos de contratación con competencias originarias, delegadas o desconcentradas, en la forma regulada en el capítulo II.

En todo caso, los órganos de contratación de la Administración General del Estado, sus Organismos autónomos, Entidades gestoras y Servicios comunes de la Seguridad Social y demás Entidades públicas estatales deberán publicar en esta plataforma su Perfil de Contratante.

Igualmente, podrán publicar información contractual la Junta Consultiva de Contratación Administrativa del Estado y los organismos similares de las Comunidades Autónomas, así como los órganos con competencias en materia de ordenación de la contratación pública, de acuerdo con lo previsto en el capítulo III.

Artículo 2. *Aprobación de especificaciones técnicas.*

Las especificaciones de contenidos y formatos serán las correspondientes a la arquitectura de información CODICE que se detalla en el Anexo III.

Las especificaciones de los protocolos de comunicación serán las recogidas en el Anexo IV.

CAPÍTULO II

Publicación del Perfil de Contratante en la Plataforma de Contratación del Estado

Artículo 3. *Alta del Perfil de Contratante.*

El alta del Perfil de Contratante deberá solicitarse por el titular de los órganos de contratación unipersonales, o por el Presidente en el caso de órganos de contratación de carácter colegiado, remitiendo a la Subdirección General de Coordinación de la Contratación Electrónica la correspondiente petición acompañada del formulario contenido en el anexo I debidamente cumplimentado.

A la solicitud se acompañará la documentación que acredite la competencia para contratar del órgano de contratación (norma legal o reglamentaria o disposición estatutaria, donde figure atribuida la facultad de celebrar contratos, normas de delegación o desconcentración de competencias en el caso de que se trate de órganos administrativos o de entes, organismos o entidades de derecho público, o poderes otorgados cuando se trate de órganos societarios o de una fundación).

La modificación de los datos del anexo I podrá hacerse por medio de escrito dirigido a la Plataforma de Contratación por el titular de los órganos de contratación unipersonales, o por el Presidente en el caso de órganos de contratación de carácter colegiado, o a través del Portal, en la forma señalada en el apartado séptimo.

Artículo 4. *Sistemas para la interacción con la Plataforma de Contratación del Estado.*

La interacción del órgano de contratación con la Plataforma de Contratación del Estado, a efectos de la publicación de la información relativa a licitaciones, podrá efectuarse a través del Portal o a través de los Servicios web definidos al efecto y publicados en la propia Plataforma, en la forma prevista en los artículos sexto y séptimo.

La información contractual de carácter general, no vinculada a procedimientos concretos de adjudicación, se enviará a la Plataforma a través del Portal, por correo electrónico o por medio de escrito.

Artículo 5. *Servicios prestados por la Plataforma de Contratación del Estado.*

1. Servicios generales. La Plataforma de Contratación del Estado prestará, con carácter general, los siguientes servicios:

a) Publicación de información contractual:

1.1 Relativa a licitaciones concretas y acuerdos marco:

1.1.1 Anuncios:

1.1.1.1 Licitación.
1.1.1.2 Adjudicación provisional.
1.1.1.3 Adjudicación definitiva.
1.1.1.4 Contrataciones programadas: anuncio indicativo previo y otras.

1.1.2 Otra información contractual:

1.1.2.1 Pliegos.
1.1.2.2 Anulación del procedimiento.
1.1.2.3 Consultas formuladas y respuestas aportadas por el órgano de contratación.

1.2 No vinculada a una licitación:

1.2.1 Celebración de acuerdos marco.
1.2.2 Instrucciones internas de contratación.
1.2.3 Modelos de Pliegos particulares para categorías de contratos de naturaleza análoga.

b) Envío de anuncios a diarios oficiales:

BOE. Se efectuará mediante los servicios Web definidos en el documento de especificación de integración de servicios descrito en el anexo IV (el pago del anuncio deberá gestionarse por el órgano de contratación).

DOUE.

c) Servicios de notificación a candidatos o licitadores:

1. Admisión y rechazo de candidatos y los licitadores.
2. Adjudicación provisional.
3. Adjudicación definitiva.
4. Renuncia del órgano de contratación a celebrar un contrato ya convocado.
5. Desistimiento del procedimiento.

d) Sellado de tiempo a través de la FNMT de todos los documentos publicados en la Plataforma, para garantizar de manera fehaciente el momento de inicio de la difusión pública de la información.

2. Sistema para las comunicaciones relativas a las licitaciones. En la interacción con la Plataforma de Contratación del Estado a través del Portal el órgano de contratación podrá utilizar el sistema de generación de anuncios, comunicaciones y notificaciones en los procesos de publicaciones de las licitaciones.

Artículo 6. *Interacción a través de Servicios Web.*

En la interacción con la Plataforma de Contratación del Estado mediante Servicios web, el órgano de contratación comunica en modo sistema a sistema la información que deba ser publicada en la Plataforma en formato CODICE, sistema basado en la transmisión de mensajes según estándar XML.

Tanto los Servicios web como todos los elementos que constituyen CODICE (plantillas, listas genéricas de código, esquemas, etc.) serán publicados y actualizados en el propio Portal.

La comunicación con la Plataforma de Contratación del Estado se realizará de forma segura mediante el uso de certificados electrónicos, según lo estipulado en el anexo IV.

Artículo 7. *Interacción a través del Portal.*

1. Usuarios del órgano de contratación. La interacción del órgano de contratación con la Plataforma de Contratación del Estado a través del Portal se efectuará por los siguientes usuarios, que tendrán las funciones que se señalan en este artículo:

Responsable del órgano de contratación, que será el titular de los órganos de contratación unipersonales o el Presidente de los órganos de contratación de carácter colegiado. El Responsable podrá realizar todas las funciones contempladas en este apartado relativas a la gestión de usuarios (altas y bajas), gestión de espacios de licitación (creación, asignación y reasignación) y gestión de la información contractual (edición y publicación), así como la modificación de los datos correspondientes al perfil del contratante.

Administrador del órgano de contratación, que podrá realizar las funciones correspondientes a la gestión de usuarios (altas y bajas) en relación con los Publicadores y Editores y la asignación y reasignación de espacios de licitación.

Publicador, que podrá realizar funciones de gestión de espacios de licitación (creación, asignación y reasignación en relación con Editores) y de gestión de la información contractual (edición y publicación).

Editor, podrá realizar funciones de edición de la información contractual, preparando la correspondiente documentación, pero sin capacidad para publicarla.

El acceso a la Plataforma por parte de estos usuarios se efectuará usando los correspondientes identificador de usuario y palabra de paso, o un certificado digital de los que se acuerde la admisión general en el ámbito de la Administración General del Estado, de acuerdo con lo establecido en los artículos 17 a 20 de la Ley 11/2007.

2. Alta y baja de Usuarios. El alta del Responsable se efectuará por la Subdirección General de Coordinación de la Contratación Electrónica. A estos efectos, cuando el órgano de contratación pretenda interactuar con la Plataforma de Contratación del Estado a través del Portal, junto con la solicitud de alta y el formulario del anexo I, deberá también remitirse el formulario del anexo II con los datos del Responsable. La Subdirección General de Coordinación de la Contratación Electrónica confirmará el alta del Responsable y le remitirá las correspondientes credenciales para acceso a la Plataforma.

El alta y la baja del Administrador deberán efectuarse por el Responsable del órgano de contratación por escrito dirigido a la Subdirección General de Coordinación de la Contratación Electrónica. Al escrito de alta deberá acompañarse el formulario recogido en el anexo II debidamente cumplimentado. La Subdirección General de Coordinación de la Contratación Electrónica confirmará el alta del Administrador y le remitirá las correspondientes credenciales para acceso a la Plataforma.

El alta y la baja de Publicador/es y Editor/es podrá realizarse por el Responsable o por el Administrador del órgano de contratación, accediendo electrónicamente al Portal y cumplimentando los correspondientes formularios.

Para que pueda procederse a la baja de usuarios que tengan asignadas licitaciones abiertas, deberá seguirse previamente el proceso de reasignación de espacios de licitación y proceder a su atribución a otro usuario.

3. Gestión de la información contractual relativa a licitaciones concretas. La gestión de la información contractual se efectuará a través de los espacios de trabajo donde el órgano de

contratación introduce y gestiona los datos necesarios para generar los anuncios, comunicaciones y notificaciones que se deben producir durante los procesos de licitación

La creación de los espacios de trabajo a efectos de generar y publicar anuncios indicativos previos o los anuncios, comunicaciones y notificaciones necesarios para la tramitación de licitaciones concretas podrá ser efectuada por el Responsable o por los Publicadores. Su asignación o reasignación podrán realizarse por el Responsable, en relación con los Publicadores y Editores, y por los Publicadores con respecto a los Editores. El Administrador podrá también proceder a la reasignación de espacios virtuales.

Artículo 8. *Baja del perfil de contratante.*

La baja voluntaria del perfil de contratante, en los casos en que el órgano de contratación no tenga obligación de publicarlo en la Plataforma de Contratación del Estado, deberá solicitarse por el responsable del órgano de contratación, por medio de escrito dirigido a la Subdirección General de Coordinación de la Contratación Electrónica.

En caso de revocación de poderes o delegaciones de competencias que priven de competencia para contratar a un órgano de contratación, la baja deberá solicitarse, por escrito, por el órgano que efectúe tal revocación.

Artículo 9. *Reorganización de unidades.*

En caso de supresión de órganos, la baja del perfil de contratante del órgano suprimido se efectuará en virtud de comunicación cursada por el órgano que asuma las funciones de éste, procediéndose a la oportuna adscripción al sucesor de los espacios de licitación que se refieran a procedimientos de adjudicación en curso.

CAPÍTULO III

Publicación de información por órganos con competencias consultivas o de ordenación en materia de contratación pública

Artículo 10. *Interacción con la Plataforma a efectos de publicar otra información contractual.*

La información relevante que deba publicarse en la Plataforma de Contratación del Estado por la Junta Consultiva de Contratación Administrativa del Estado y organismos similares de las Comunidades Autónomas, así como por los órganos con competencias en materia de ordenación de la contratación pública, será remitida a la Subdirección General de Coordinación de la Contratación Electrónica para su publicación en la Plataforma.

Disposición final única. *Entrada en vigor.*

La presente Orden entrará en vigor el día 2 de mayo de 2008.

ANEXO I

Datos para el alta del perfil del contratante

Tipo de Administración: Tipo de Administración a la que pertenece el Perfil del Contratante (AGE, CC.AA., Entidad Local, etc.)

Nombre del Departamento u órgano de dependencia: Deberá especificarse el nombre del Departamento si existe dependencia (Ministerio, Secretaria de Estado, Organismo Autónomo, etc.)

Nombre del órgano de contratación: Nombre del órgano de contratación al que se le asocia el Perfil del Contratante

Rol del órgano de contratación: Se especificará el rol con el que actúa el órgano de contratación (Central de Compras, Junta de Contratación, órgano de contratación)

CIF: Numero de Identificación Fiscal que utilizará el órgano de contratación

Idioma preferente: Idioma preferente que utilizará el órgano de contratación.

URL del órgano de contratación: URL del Site del órgano de contratación como fuente de información adicional.

Actividad del órgano de contratación: Tipo de actividad del poder adjudicador (Defensa, Economía y Hacienda, Sanidad, Interior, Vivienda, Ocio, Educación, etc.). El campo admite mas de un valor.

Dirección Postal del órgano de contratación:

Nombre de la Calle.
Código Postal.
Población.
País.
Contacto del Perfil del Contratante.
Teléfono.
Fax.
Email: Dirección de correo Electrónica de la persona de contacto del órgano de contratación.

Integración con la Plataforma:

URL de Recepción de Ofertas: Dirección única que identificará el Servicio Web donde el órgano de contratación desea recibir las Ofertas recibidas a través de la Plataforma en las licitaciones electrónicas. Esta dirección será necesaria solo para aquellos casos en que el órgano de contratación posea un sistema informático propio que le permita efectuar procesos de licitación electrónica.
Tipo de Integración: Modo en el que el órgano de contratación puede integrarse con la Plataforma (Portal o Sistémica).
Certificado del órgano de contratación: En el caso de que el Tipo de integración sea sistémica, el órgano de contratación adjuntará, con la petición de alta, un fichero en Base64 con la parte pública del Certificado de componente emitido por una Autoridad de Certificación reconocida en la Administración General del Estado.

ANEXO II

Alta de un usuario

Nombre:
Apellidos:
Documento de Identificación (DNI/NIE):
Rol: Funciones que desempeñará el usuario del que se solicita el alta dentro de la Plataforma.

Según la definición de roles en la Plataforma, este campo podrá tener los siguientes valores:

ROC (responsable del órgano de contratación).
AOC (Administrador del órgano de contratación).
POC-PUB (Publicador del órgano de contratación).
POC-ED (Editor del órgano de contratación).

Cargo: Cargo que desempeña el usuario dentro del órgano de contratación.
Email: Dirección de correo Electrónica del usuario para el que se solicita el Alta.

ANEXO III

Especificaciones de contenidos y formatos correspondientes a la arquitectura de información CODICE

CODICE es una librería de componentes y documentos electrónicos estándar para el desarrollo de aplicaciones de contratación pública electrónica de conformidad con los procedimientos y prescripciones de la Directiva 2004/18 y de la Ley 30/2007, de 30 de octubre de 2007, de Contratos del Sector Público, así como con los estándares y

recomendaciones internacionales aplicables a la identificación, denominación, definición y construcción de dichos componentes.

La arquitectura desarrollada proporciona la biblioteca de componentes estándar, reutilizables, y extensibles o adaptables a diversos contextos o necesidades de contratos públicos específicos, para satisfacer las necesidades de información de los documentos y mensajes intercambiados a lo largo del ciclo completo de los procedimientos electrónicos de contratación contemplados en la citada Directiva.

Dichos componentes deberían ser además suficientes para la construcción a partir de ellos de cualquier documento o mensaje estructurado (o estructurable) intercambiado entre los participantes de un proceso de contratación pública susceptible de conversión a formato electrónico funcionalmente equivalente.

CODICE proporciona una biblioteca con los documentos electrónicos estandarizados básicos o comunes utilizados en dichos procedimientos, construidos a partir de la librería de los componentes.

La última versión de la especificación técnica de los documentos electrónicos CODICE se puede encontrar en el Portal de la Plataforma de Contratación del Estado http://contrataciondelestado.es y contempla los siguientes documentos:

1. Anuncio de licitación (ContractNotice): Documento que utiliza un órgano de contratación para anunciar el proyecto de adquisición de bienes, servicios u obras. El anuncio de licitación se publicará en el perfil del contratante y si se supera el umbral legal deberá ser publicado en otras publicaciones como el Diario Oficial de la Unión Europea.
2. Anuncio Previo (PriorInformationNotice): Documento que utiliza un órgano de contratación para declarar la intención de comprar bienes, servicios o trabajos durante un período de tiempo determinado. Se trata de un documento no vinculante que puede ser usado para declarar la voluntad de adquirir durante un período, y tiene el efecto de permitir que el órgano de contratación pueda reducir los plazos en el proceso de licitación.
3. Anuncio de Adjudicación (ContractAwardNotice): Documento publicado por un órgano de contratación para anunciar la adjudicación de un contrato.
4. Pliegos (ContractDocuments): Documento que un órgano de contratación publica o envía a un empresario para ofrecerle información acerca de un contrato en licitación. Este es el principal documento para la licitación, en él, los órganos de contratación especifican el objeto del contrato, el proceso de licitación y sus condiciones.
5. Oferta (Tender): Documento mediante el cual un licitador ofrece sus productos, servicios o proyectos como respuesta a una licitación.
6. Declaración (Declaration): Documento que utiliza el operador económico para realizar declaraciones sobre su propia condición. Se utiliza para permitir al órgano de contratación evaluar la capacidad del operador económico de participar en el proceso de licitación.
7. Garantía (Guarantee): Documento para notificar el depósito de una garantía.
8. Notificación de adjudicación (AwardNotification): Documento que se utiliza para comunicar la adjudicación del contrato al adjudicatario.
9. Notificación de no adjudicación (UnawardedNotification): Documento que se utiliza para comunicar la adjudicación del contrato a otro licitador.
10. Notificación de admisión/exclusión (QualificationResultNotification): Documento que el órgano de contratación envía a un operador económico a fin de notificarle su admisión o exclusión al proceso de licitación.
11. Notificación de recurso (AppealNotification): Documento que el órgano de contratación envía a todos los licitadores en un proceso de licitación ante la eventual presentación de un recurso por parte de uno de los licitadores.
12. Notificación de recepción de oferta (TenderReceptionNotification): Documento enviado por el órgano de contratación a un operador económico para notificar de la recepción de la oferta de licitación. Está firmado por el órgano de contratación para que el licitador obtenga una prueba de presentación.
13. Invitación a licitar (InvitationToTender): Documento enviado por el órgano de contratación a un operador económico invitándolo a presentar oferta a un proceso de licitación.
14. Solicitud de pliegos (ContractDocumentsRequest): Documento enviado por el operador económico solicitando la documentación del contrato. En algunos procesos de

licitación, los pliegos no son de acceso público, por lo que los licitadores deben solicitarlo mediante este documento

15. Solicitud de subsanación (ClarifyingRequest): Documento enviado por el órgano de contratación a un operador económico solicitando aclaraciones o nueva documentación para poder evaluarle como candidato válido para un proceso de licitación.

Toda la documentación completa necesaria para la implementación de CODICE, así como las modificaciones que pudiera producirse, de uso libre y gratuito, estará a disposición pública en el Portal de la Plataforma de Contratación del Estado (http://contrataciondelestado.es), con el contenido que se detalla a continuación:

1. Memoria CODICE:

Análisis de procedimientos de contratación: estudio de los distintos procedimientos de contratación previstos en la Directiva Europea 2004/18/CE y en la Ley de Contratos del Sector Público española

Normalización UMM de procesos de negocio: representación de los procesos de negocio y de las transacciones implicadas en la contratación electrónica.

2. Mapa ontológico: Contiene todos los componentes CODICE, más los reutilizados de UBL en un único diagrama de clases. Ensamblando estos componentes se han construido los documentos CODICE. Estos mismos componentes podrán utilizarse para crear nuevos documentos.

3. Documentos ensamblados: creados a partir de componentes, con varias representaciones de dichos documentos:

Diagramas de clases. Modelos UML de los documentos CODICE.

Modelo de datos en hoja de calculo.

Esquemas XSD v1.04. Contiene la definición de la estructura XML que deben cumplir los documentos CODICE. Se utilizan para validar los documentos CODICE.

XML de ejemplo.

Guías de implementación. Explicación de cómo implementar cada uno de los documentos CODICE.

4. Listas de códigos: Listas de valores para aquellos elementos de datos que requieren codificación.

ANEXO IV

Especificaciones de los protocolos de comunicación de información

La Plataforma de Contratación del Estado, en cumplimiento de la normativa aplicable, facilita una serie de servicios de publicación para los Órganos de Contratación de la Administración mediante un acceso Web al Portal de Contratación y mediante acceso sistémico de maquina a maquina denominado integración B2B.

Los servicios expuestos por la plataforma para la publicación sistema a sistema son los relativos a los siguientes casos de uso:

1. Solicitud de publicación de anuncios y pliegos:

a) Publicación del Anuncio Previo
b) Publicación del Anuncio del Licitación
c) Publicación del Documento de Pliego
d) Publicación del Anuncio de Adjudicación

2. Solicitud de estado de un Espacio Virtual de Licitación (EVL). El EVL es un concepto que maneja la Plataforma y que se equipara al conjunto de datos del expediente (interno al órgano de contratación) al que hay que dar publicidad.

3. Reenvío de las Ofertas recibidas en la Plataforma de contratación a los sistemas de los Órganos de Contratación.

Como mecanismo de comunicación sistema a sistema entre la Plataforma de Contratación del Estado y los Órganos de Contratación se utiliza tecnología Web Services con las siguientes características:

Uso de mensajería SOAP sobre un transporte síncrono petición/respuesta como http(s).

Definición de servicios mediante el lenguaje de definición de servicios Web WSDL.

Uso de canal cifrado mediante SSL/TLS (https) para preservar la confidencialidad de la información antes de su publicación.

La autenticación de los Órganos de Contratación en la plataforma se realizará mediante la utilización de WebService Security (WS-S). El órgano de contratación firmará las peticiones mediante un Certificado Digital de una Autorizada de Certificación (CA) reconocida, del cual debe facilitarse a la plataforma su parte pública (según se especifica en el anexo I).

La última versión de la especificación técnica de los protocolos de comunicación para el intercambio de contenidos sistema a sistema se puede encontrar en Portal de la Plataforma de Contratación del Estado http://contrataciondelestado.es y consta de los siguientes documentos:

1. Documento de Especificación de Integración de Servicios sistema a sistema (B2B).
2. Documento de Especificación de Reenvío de Oferta mediante mecanismos sistema a sistema (B2B).

Cualquier otro documento que deba utilizarse en nuevas implementaciones, o las modificaciones que puedan producirse en los existentes, será puesto a disposición de los interesados en el portal de la Plataforma de Contratación del estado en la dirección http://contrataciondelestado.es

§ 16

Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social

Ministerio de Empleo y Seguridad Social
«BOE» núm. 75, de 28 de marzo de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-3362

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, insta en su artículo 45.1 a las administraciones públicas a impulsar el uso y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de dichos medios establecen la Constitución y las leyes. Por su parte, el derecho de los ciudadanos a comunicarse con las administraciones por medios electrónicos se consagra con la promulgación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en la que se regula la actuación de las administraciones públicas para generalizar la sociedad de la información a través de dichos medios. En desarrollo de esta última ley, el Real Decreto 1671/2009, de 6 de noviembre, establece un marco flexible para facilitar la adaptación de organizaciones, funciones y procedimientos a la comunicación por medios electrónicos, garantizando al mismo tiempo que no resulten afectados otros bienes constitucionalmente protegidos, como son la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros.

Dentro del ámbito específico de la Administración de la Seguridad Social el uso y aplicación de técnicas y medios electrónicos para el desarrollo de su actividad y el ejercicio de sus competencias se ha regulado en la Orden de 3 de abril de 1995, sobre uso de medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, la afiliación, altas y bajas de trabajadores, la cotización y la recaudación; medios y procedimientos que, bajo la denominación «Sistema de remisión electrónica de datos (Sistema RED)», han sido objeto de implantación y desarrollo progresivo a través de sucesivas resoluciones de la Dirección General de la Tesorería General de la Seguridad Social, dictadas en aplicación de la referida Orden ministerial.

El alcance y las condiciones de utilización del Sistema RED se han ido perfilando, asimismo, al amparo de lo previsto en el artículo 30 de la Ley 50/1998, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, en aplicación del cual, por una parte, la Orden TAS/399/2004, de 12 de febrero, sobre presentación en soporte informático de los partes médicos de baja, confirmación de la baja y alta correspondientes a procesos de incapacidad temporal, ha extendido su ámbito de aplicación a la presentación de partes médicos de baja, confirmación de baja y alta correspondientes a procesos de incapacidad temporal, y, por otra parte, por la Orden TAS/1562/2005, de 25 de mayo, por la que se

establecen normas para la aplicación y desarrollo del Reglamento general de recaudación de la Seguridad Social, se determinaron los supuestos de incorporación obligatoria a dicho sistema, tras su reforma por la Orden TIN/2777/2010, de 29 de octubre, y recientemente en el ámbito del Régimen Especial del Mar se ampliaron esos supuestos por Orden ESS/229/2012, de 9 de febrero, por la que se establecen para el año 2012 las bases de cotización a la Seguridad Social de los trabajadores del Régimen Especial del Mar incluidos en los grupos segundo y tercero.

A su vez, diversas normas reglamentarias de Seguridad Social, tales como la disposición adicional quinta del Reglamento general de la gestión financiera de la Seguridad Social, aprobado por el Real Decreto 1391/1995, de 4 de agosto; la disposición adicional sexta del Reglamento general sobre cotización y liquidación de otros derechos de la Seguridad Social, aprobado por el Real Decreto 2064/1995, de 22 de diciembre; el artículo 38 del Reglamento general sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social, aprobado por el Real Decreto 84/1996, de 26 de enero y las disposiciones adicionales cuarta y quinta del Reglamento general de recaudación de la Seguridad Social, aprobado por el Real Decreto 1415/2004, de 11 de junio, también contemplan la posibilidad de utilizar los procedimientos y medios que conforman el Sistema RED para la realización de actuaciones administrativas y el suministro de datos o documentos relativos a las materias reguladas por tales reglamentos, quedando habilitada la Ministra de Empleo y Seguridad Social para determinar las condiciones de uso del citado sistema, bien de forma expresa en esos mismos preceptos o bien mediante las correspondientes disposiciones finales sobre facultades de aplicación y desarrollo de los respectivos reglamentos.

Finalmente, la disposición adicional quincuagésima del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto legislativo 1/1994, de 20 de junio, ha introducido la obligatoriedad de notificación por medios electrónicos, informáticos o telemáticos de los actos administrativos que traigan causa o se dicten como consecuencia de los datos transmitidos electrónicamente a través del Sistema RED.

En base a las referidas previsiones legales y con el objetivo de sistematizar los criterios en ellas establecidos, así como prever la extensión de la obligatoriedad de incorporación a dicho sistema al resto de las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar encuadrados en cualquiera de los regímenes del sistema de la Seguridad Social, con independencia del número de trabajadores que mantengan en alta, se considera conveniente regular en un texto único la utilización de medios electrónicos, informáticos y telemáticos en las actuaciones de inscripción de empresas, afiliación, altas, bajas y variaciones de datos de trabajadores, cotización y recaudación de empresas y trabajadores, comunicación de partes médicos de baja, de confirmación de la baja y alta correspondiente a procesos de incapacidad temporal, así como cualquier otra actuación que se determine en el ámbito de la Seguridad Social a través del Sistema RED.

Esta orden ha sido informada favorablemente por la Comisión Ministerial de Administración Electrónica del Ministerio de Empleo y Seguridad Social, al amparo de lo previsto por el artículo 2.2.e) de la Orden TIN/3155/2011, de 8 de noviembre, por la que se regula la composición y funciones del citado órgano colegiado.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, y de acuerdo con el Consejo de Estado, dispongo:

Artículo 1. *Objeto y ámbito de aplicación objetivo.*

1. Esta orden tiene por objeto regular el Sistema de remisión electrónica de datos (en adelante, Sistema RED), como un servicio gestionado por la Tesorería General de la Seguridad Social para el intercambio electrónico de datos o documentos, así como para la comunicación de actuaciones administrativas entre ésta y los autorizados para ello, con el fin de facilitar el cumplimiento de las obligaciones de Seguridad Social por parte de los sujetos responsables en las siguientes materias:

a) Inscripción de empresas, afiliación, altas, bajas y variaciones de datos de trabajadores, cotización y recaudación de empresas y trabajadores en el ámbito de la

Seguridad Social en los términos y condiciones previstos en cada momento por la normativa aplicable a estas materias.

b) Comunicación de partes médicos de baja, de confirmación de la baja y de alta correspondiente a procesos de incapacidad temporal cuya gestión esté encomendada a la entidad gestora o a la mutua de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, en los términos establecidos en la Orden TAS/399/2004, de 12 de febrero, sobre presentación en soporte informático de los partes médicos de baja, confirmación de la baja y alta correspondientes a procesos de incapacidad temporal.

c) Cualquier otra actuación que venga exigida en la normativa de la Seguridad Social, cuya gestión venga atribuida a la Tesorería General de la Seguridad Social en la forma y con las especificaciones técnicas que establezca por resolución de su Director General.

2. Las notificaciones de los actos administrativos que traigan causa o se dicten como consecuencia de los datos que deban comunicarse electrónicamente a través del Sistema RED se efectuarán en la sede electrónica de la Secretaría de Estado de la Seguridad Social, de acuerdo con lo previsto en la disposición adicional quincuagésima del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto legislativo 1/1994, de 20 de junio, así como en la Orden ESS/485/2013, de 26 de marzo, por la que se regulan las notificaciones y comunicaciones por medios electrónicos en el ámbito de la Seguridad Social.

Artículo 2. *Ámbito de aplicación subjetivo.*

1. La incorporación al Sistema RED será obligatoria para los sujetos responsables de la obligación de cotizar a que se refiere el apartado 2 de este artículo. Los restantes sujetos responsables podrán incorporarse voluntariamente para la realización de los trámites administrativos que en cada momento permita dicho sistema para estos colectivos. En todo caso se precisará para la incorporación la autorización previa otorgada por la Tesorería General de la Seguridad Social.

2. A los efectos indicados, las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar encuadrados en cualquiera de los regímenes del sistema de la Seguridad Social, con independencia del número de trabajadores que mantengan en alta, estarán obligados a su incorporación al Sistema RED, sin perjuicio de lo establecido en los párrafos siguientes.

En el caso de los trabajadores incluidos en el Régimen Especial de la Seguridad Social de los Trabajadores por Cuenta Propia o Autónomos, con excepción de los correspondientes al Sistema Especial de Trabajadores por Cuenta Propia Agrarios, sólo estarán obligados a su incorporación efectiva al Sistema RED los que al mismo tiempo tengan la condición de empresarios obligados a transmitir por dicho sistema los datos relativos a sus trabajadores, en cuyo caso también estarán obligados a transmitir por el mismo sistema sus propios datos como trabajadores autónomos.

La incorporación al Sistema RED no será obligatoria para las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar encuadrados en el Régimen General, por lo que respecta a los colectivos de profesionales taurinos y representantes de comercio y a los Sistemas Especiales para Empleados de Hogar y de la Industria Resinera, así como en el Régimen Especial de los Trabajadores del Mar, respecto a los trabajadores por cuenta propia.

3. Las actuaciones administrativas, para el intercambio de datos o documentos, en el Sistema RED podrán llevarse a cabo por los sujetos responsables del cumplimiento de las obligaciones a que se refiere el artículo 1, bien en nombre propio o bien por medio de representante.

Artículo 3. *Incidencia de la incorporación efectiva al Sistema RED en la adquisición y mantenimiento de beneficios en la cotización a la Seguridad Social.*

1. Conforme a lo previsto en el párrafo primero del artículo 29 de la Ley 50/1998, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, en el caso de que las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar que hubieran solicitado u obtenido reducciones, bonificaciones o

cualesquiera otros beneficios en las bases, tipos y cuotas de la Seguridad Social y conceptos de recaudación conjunta, no se incorporen de manera efectiva al Sistema RED, no podrán obtener los citados beneficios y quedarán suspendidos, sin más trámite, los que tuvieran concedidos, respecto de todos sus trabajadores por cuenta ajena o asimilados y respecto de todos sus códigos de cuenta de cotización, tanto principales como secundarios, desde la fecha en que tal incorporación debió realizarse. Dicha suspensión se aplicará, asimismo, a los sujetos responsables que dejen de utilizar de forma efectiva el Sistema RED en las actuaciones relativas al encuadramiento, cotización y recaudación.

La obtención de los beneficios indicados se regirá por la normativa vigente en el período de liquidación correspondiente a la incorporación efectiva al Sistema RED y surtirá efectos desde el día primero de dicho período, sin perjuicio de la pérdida de los beneficios por el tiempo transcurrido desde el nacimiento del derecho hasta tal incorporación efectiva. Asimismo, la suspensión de aquellos beneficios quedará sin efecto y volverán a ser aplicables a partir de la liquidación correspondiente a la nueva incorporación a dicho sistema, sin que quepa la recuperación de los beneficios perdidos. Tanto en un caso como en otro, se considerará que los beneficios se han aplicado, a efectos del cómputo de su duración, durante el periodo transcurrido entre la fecha inicial en que se hubiesen podido obtener, se hubiesen obtenido o se hubiesen suspendido, y la de incorporación efectiva al Sistema RED.

No dará lugar a la pérdida de reducciones, bonificaciones o cualesquiera otros beneficios que tuvieran concedidos, la falta de transmisión de datos a través del Sistema RED por causas de carácter técnico imputables a la Tesorería General de la Seguridad Social, sin perjuicio de la obligación de presentar los documentos de cotización y los de afiliación, altas, bajas y variaciones de datos dentro de los plazos establecidos.

2. A los efectos previstos en el apartado anterior, se entiende por incorporación efectiva al Sistema RED la utilización de dicho sistema para la realización de las actuaciones previstas en el artículo 1 con plena validez y eficacia, generando los derechos y obligaciones establecidos por la normativa en vigor en relación con dichos actos, así como de cualesquiera otras exigidas en la normativa de Seguridad Social, en la forma y con los requerimientos que fije la Tesorería General de la Seguridad Social.

3. El cumplimiento de la obligación de incorporación al Sistema RED no se verá afectado cuando las actuaciones de encuadramiento, cotización y recaudación puedan realizarse a través de otros medios electrónicos distintos del citado sistema, en los términos y condiciones que fije la Tesorería General de la Seguridad Social, a fin de facilitar la prestación de los servicios electrónicos en aplicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Artículo 4. *Características del Sistema RED.*

1. El Sistema RED comprenderá las aplicaciones informáticas y telemáticas que en cada momento resulten precisas para el cumplimiento de la finalidad antes indicada, autorizándose a tal efecto la utilización de redes públicas y privadas de transmisión de datos, combinaciones de unas y otras y cualesquiera otros medios que determine la Tesorería General de la Seguridad Social.

2. El Sistema RED garantiza los siguientes principios generales:

a) Autenticación. El sistema identificará de manera inequívoca al emisor y al receptor de la información que sea distinto de la Tesorería General de la Seguridad Social, asegurando su identidad. La identificación de los interesados necesariamente se efectuará mediante sistemas de firma electrónica determinados conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como en los artículos 13 y siguientes de la Ley 11/2007, de 22 de junio, y en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada ley, que resulten adecuados para garantizar su identificación, así como la autenticidad de los documentos electrónicos.

b) Constancia. El sistema dispondrá de un servicio en el que se haga constar la fecha y hora de envío de cada una de las comunicaciones realizadas entre los usuarios y la Tesorería General de la Seguridad Social.

c) Confidencialidad. El sistema garantizará que sólo el usuario acreditado debidamente tenga acceso a las comunicaciones que contengan datos de carácter personal, de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A tal efecto, el sistema incluirá las pertinentes medidas de seguridad en las transmisiones mediante el cifrado de datos o a través de cualquier otro mecanismo que garantice que la información no es inteligible ni manipulable por terceros.

d) Integridad. El sistema garantizará que la información y documentos serán transmitidos sin alteración alguna de su contenido original, pudiendo ser detectada cualquier anomalía por el receptor de los mismos.

e) Conservación. El sistema garantizará la conservación de la información y documentos transmitidos durante el tiempo exigido por la normativa aplicable en función de los datos transmitidos.

f) No repudio. El sistema se instrumentará de forma que el receptor de la información o documento no pueda rechazar un envío válidamente efectuado y que el remitente tenga constancia de su recepción.

Artículo 5. *Autorización para actuar a través del Sistema RED.*

1. Para operar en el ámbito de actuación definido en el artículo 1, será necesario contar con autorización otorgada por la Tesorería General de la Seguridad Social. Dicha autorización podrá ser de dos tipos:

a) Autorización para actuar en nombre propio.

b) Autorización para actuar en nombre de otros.

La Tesorería General de la Seguridad Social determinará mediante resolución del Director General los requisitos que se han de cumplir para la obtención de cada tipo de autorización.

2. Las solicitudes de autorización serán resueltas por los directores provinciales de la Tesorería General de la Seguridad Social, informándose al autorizado de las condiciones de utilización de la autorización en el caso de resoluciones estimatorias.

El plazo máximo en que debe notificarse la resolución expresa será de tres meses, transcurrido dicho plazo podrá entenderse desestimada la solicitud por silencio administrativo.

Dicha resolución podrá ser objeto de recurso de alzada ante la Dirección General de la Tesorería General de la Seguridad Social, de acuerdo con lo establecido en los artículos 114 y 115 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya interposición suspenderá la ejecución del acto impugnado. El plazo para la interposición de dicho recurso será el de un mes a contar desde el día siguiente a la notificación. Transcurrido el plazo de tres meses desde la interposición de dicho recurso de alzada sin que recaiga resolución expresa, el mismo podrá entenderse desestimado, según dispone el artículo 115 de la citada Ley 30/1992, de 26 de noviembre.

Las autorizaciones concedidas dejarán de surtir efectos tanto por incumplimiento de sus condiciones de utilización como por el uso abusivo o fraudulento de éstas, mediante resolución motivada de la Tesorería General de la Seguridad Social.

3. Concedida una autorización para actuar a través del Sistema RED, el autorizado quedará habilitado tanto para la transmisión electrónica de los datos o documentos a través del referido sistema como para la recepción de las comunicaciones y notificaciones de las actuaciones administrativas que se realicen al respecto, implicando esta autorización la obligación del autorizado de gestionar con carácter exclusivo mediante dicho sistema, salvo imposibilidad del servicio por causa debida a la Tesorería General de la Seguridad Social, el cumplimiento de las obligaciones y actuaciones en las materias a que se refiere el artículo 1 respecto de todos los sujetos responsables vinculados a dicha autorización, entendiéndose realizadas directamente por estos últimos.

4. Las actuaciones a las que habilita la autorización RED para la transmisión electrónica de datos o documentos y recepción de las comunicaciones y notificaciones de las actuaciones administrativas consecuencia de dicha transmisión, podrán ser realizadas tanto por el autorizado como por los usuarios que éste designe a través del correspondiente

servicio establecido al efecto por la Tesorería General de la Seguridad Social, garantizándose conforme al artículo 4.2.a) la identificación del emisor o receptor y la autenticidad e integridad de los datos y documentos objeto de transmisión.

En todo caso, las transmisiones de datos o documentos realizadas por los usuarios a través del Sistema RED, así como las comunicaciones y las notificaciones de las actuaciones administrativas que éstos reciban de la Tesorería General de la Seguridad Social, se entenderán transmitidos y recibidos por el autorizado.

Artículo 6. *Requisitos para el ejercicio efectivo de las autorizaciones RED.*

Para el intercambio efectivo de los datos o documentos y recepción de las comunicaciones y notificaciones de las actuaciones administrativas que traigan causa o se dicten como consecuencia de los datos que deban comunicarse a través del Sistema RED, correspondientes a sujetos responsables, se requiere:

a) En el caso de autorizaciones para actuar en nombre propio, la comunicación por el medio que establezca al efecto la Tesorería General de la Seguridad Social de los códigos de cuenta de cotización o números de afiliación cuyos datos hayan de ser transmitidos a través del Sistema RED.

b) En el caso de autorizaciones para actuar en nombre de terceros, además de la comunicación a que se refiere el párrafo anterior, será necesaria la acreditación de la representación otorgada por los sujetos responsables en cuyo nombre se actúe, a favor del autorizado y de sus usuarios, por el medio que establezca la Tesorería General de la Seguridad Social.

Artículo 7. *Responsabilidad de los autorizados.*

La responsabilidad de las actuaciones realizadas recae en todo caso sobre el autorizado, con independencia de quien las efectúe, y sin perjuicio de la responsabilidad que éste pueda exigir a los usuarios responsables de la actuación.

Se prohíbe expresamente al autorizado RED y a los usuarios designados por éste el tratamiento automatizado de los datos a los que tengan acceso mediante la creación de ficheros informáticos para fines distintos de los estrictamente propios del Sistema RED.

Será responsabilidad del autorizado mantener actualizada la relación de usuarios acreditados a operar en el sistema, en el marco de su autorización.

Artículo 8. *Efectos de la transmisión electrónica de datos o documentos a través del Sistema RED.*

1. La remisión electrónica de datos o documentos relativos a actuaciones de inscripción de empresas, afiliación, altas, bajas y variaciones de datos de trabajadores, cotización y recaudación de empresas y trabajadores en el ámbito de la Seguridad Social y la comunicación de partes médicos de baja, de confirmación de la baja y de alta correspondientes a procesos de incapacidad temporal a través del Sistema RED, así como la transmisión de las actuaciones administrativas realizadas por la Tesorería General de la Seguridad Social o entidad gestora correspondiente, que se deriven de la citada transmisión, gozarán de plena validez y eficacia, generando los derechos y obligaciones establecidos por la normativa en vigor en relación con dichos actos.

2. La obligación de informar sobre los datos figurados en las relaciones nominales de trabajadores (documentos serie TC-2) que se transmitan por el Sistema RED, prevista en el artículo 25.4 del Reglamento general de recaudación de la Seguridad Social, aprobado por el Real Decreto 1415/2004, de 11 de junio, se considerará cumplida de acuerdo con lo dispuesto en dicho artículo, mediante la colocación o puesta a disposición de los trabajadores, a través de la presentación en pantalla de ordenador o terminal informático, de los datos de sus archivos que, a tales efectos, serán considerados como copia autorizada de las citadas relaciones nominales de trabajadores, siempre que, en este último caso, se muestren acompañados de su correspondiente huella electrónica.

3. En el supuesto de falta de ingreso de las obligaciones de pago correspondientes, la aportación en soporte informático de los datos de las relaciones nominales de trabajadores efectuada en plazo reglamentario se considerará como presentación de documentos de

cotización a los efectos previstos en el artículo 26 del texto refundido de la Ley General de la Seguridad Social.

4. La utilización del Sistema RED para el suministro de datos se entenderá sin perjuicio del cumplimiento, por parte de las empresas y demás sujetos responsables, de las demás obligaciones previstas en el Reglamento general sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social, aprobado por el Real Decreto 84/1996, de 26 de enero.

Artículo 9. *Validez de los documentos generados por impresión autorizada de las actuaciones tramitadas electrónicamente a través del Sistema RED.*

Los documentos generados por impresión autorizada de las actuaciones tramitadas electrónicamente a través del Sistema RED incluirán elementos de contraste/cotejo y gozarán de la misma validez y eficacia frente a terceros que las certificaciones expedidas al respecto por los órganos competentes de la Tesorería General de la Seguridad Social.

La Tesorería General de la Seguridad Social podrá realizar la impresión de los datos y documentos recibidos, producidos y emitidos por el Sistema RED, considerándose como impresión de contraste y gozando de la misma validez que los originales tramitados.

La autenticidad e integridad de los documentos generados podrá verificarse mediante los sistemas dispuestos a tal efecto, consistentes en la verificación mediante el código electrónico de autenticidad (CEA), mediante huella digital o cualquier otro sistema que permita contrastar la información de dichos documentos con la obrante en las correspondientes bases de datos corporativas.

Artículo 10. *Conexión y modalidades de trabajo.*

1. La conexión para el intercambio electrónico de datos o documentos se realizará a través de internet.

Excepcionalmente, la Tesorería General de la Seguridad Social podrá autorizar a determinados sujetos responsables con un elevado número de trabajadores, a optar por una modalidad de intercambio electrónico de datos bajo protocolo «ad hoc». Asimismo, por la Tesorería General de la Seguridad Social podrá determinarse igualmente, en función de otros criterios objetivos, qué autorizados utilizarán un determinado protocolo para el intercambio de datos.

2. Las modalidades de trabajo utilizadas por el Sistema RED son dos:

a) Conexión directa con la Tesorería General de la Seguridad Social.

b) Envío y recepción de ficheros con una estructura determinada, según instrucciones técnicas que figuran en la página web de la Seguridad Social.

La Tesorería General de la Seguridad Social podrá incluir cualquier otro protocolo o modalidad de trabajo que la evolución tecnológica aconseje, así como la supresión de los utilizados hasta el momento.

Disposición adicional primera. *Exención de la obligación de presentación de la relación nominal de trabajadores.*

En aquellos supuestos en los que existiendo transmisión electrónica de la relación nominal de trabajadores a través del Sistema RED, y por razones técnicas la Tesorería General de la Seguridad Social no pueda calcular la liquidación correspondiente, no será necesario adjuntar, para su sellado y validación, dicha relación nominal de trabajadores (documentos serie TC-2) al boletín de cotización (serie TC-1) en el momento del ingreso de las cuotas en cualquiera de las oficinas recaudadoras autorizadas. Al respecto, en la casilla del boletín de cotización (serie TC-1) reservada a firma y sello del empresario se indicará:

«No acompaña TC-2

Autorización TGSS número..... de fecha.....»

Disposición adicional segunda. *Servicio de asistencia y orientación para la cumplimentación de las actuaciones de encuadramiento, cotización y recaudación por medios electrónicos.*

En el marco de lo previsto por el artículo 8 de la Ley 11/2007, de 22 de junio, la Tesorería General de la Seguridad Social pondrá a disposición de las empresas, agrupaciones de empresas y demás sujetos responsables obligados a incorporarse de manera efectiva al Sistema RED, que por sus dificultades personales o su reducida dimensión y localización geográfica así lo requieran, un servicio de asistencia técnica y asesoramiento, que incluirá los medios necesarios para garantizar la efectividad del cumplimiento de la obligación de transmisión electrónica de los datos de encuadramiento, cotización y recaudación impuesta por el artículo 1.1.

Dicho servicio se prestará siempre que el sujeto responsable no disponga de la correspondiente autorización para transmitir por el Sistema RED, en los términos y condiciones que determine la Tesorería General de la Seguridad Social.

Disposición transitoria única. *Autorizaciones para actuar a través del Sistema RED otorgadas con anterioridad a la fecha de entrada en vigor de esta orden.*

Respecto a las autorizaciones para actuar a través del Sistema RED otorgadas con anterioridad a la fecha de entrada en vigor de esta orden a profesionales colegiados y terceros que viniesen transmitiendo electrónicamente a través del Sistema RED datos relativos a una o varias empresas, agrupaciones de empresas y demás sujetos responsables, serán válidas, salvo manifestación expresa en contrario, y sin perjuicio de que la Tesorería General de la Seguridad Social pueda en cualquier momento solicitar la acreditación de la representación, procediendo a dejar sin efecto la autorización respecto de las empresas o sujetos obligados en el caso de que no se acredite suficientemente ésta.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas todas las disposiciones de igual o inferior rango en tanto contradigan o se opongan a lo establecido en esta orden.

2. Quedan derogadas expresamente las siguientes disposiciones:

a) La Orden de 3 de abril de 1995, sobre uso de medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, afiliación, altas y bajas de trabajadores, cotización y recaudación en el ámbito de la Seguridad Social.

b) De la Orden TAS/1562/2005, de 25 de mayo, por la que se establecen normas para la aplicación y desarrollo del Reglamento general de recaudación de la Seguridad Social, aprobado por el Real Decreto 1415/2004, de 11 de junio, el artículo 28 y las disposiciones adicionales cuarta y quinta.

c) De la Orden ESS/229/2012, de 9 de febrero, por la que se establecen para el año 2012 las bases de cotización a la Seguridad Social de los trabajadores del Régimen Especial del Mar incluidos en los grupos segundo y tercero, los apartados 1 y 2 de su disposición adicional única.

Disposición final primera. *Título competencial.*

Esta orden se dicta al amparo de lo dispuesto en el artículo 149.1.17.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de legislación básica y régimen económico de la Seguridad Social.

Disposición final segunda. *Facultades de aplicación y desarrollo.*

Se faculta al Director General de la Tesorería General de la Seguridad Social para dictar cuantas resoluciones resulten necesarias para la aplicación de lo dispuesto en esta orden.

Disposición final tercera. *Entrada en vigor.*

La presente orden entrará en vigor el día 1 del mes siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 17

Resolución de 21 de marzo de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Guía de Comunicación Digital para la Administración General del Estado

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 79, de 2 de abril de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-3528

En los últimos años, la comunicación con los ciudadanos y las empresas por medios digitales a través de portales web, sedes electrónicas, blogs, o redes sociales, a los que en adelante en esta resolución se denominarán bajo el término genérico de sitios web, ha adquirido una importancia indiscutible para la Administración General del Estado (AGE) conformándose como una herramienta indispensable para la difusión de sus contenidos y para fortalecer la participación ciudadana e impulsar la transparencia de la actividad pública.

Además, cabe recordar que como consecuencia de la aplicación de la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos y del Título II del Real Decreto 1671/2009, de 6 de noviembre, de desarrollo parcial de dicha Ley, la AGE ofrece actualmente la tramitación electrónica de la práctica totalidad de los servicios administrativos en sus sedes electrónicas.

Los estudios sobre el uso en un futuro próximo de los sitios web de las administraciones públicas coinciden en señalar que su utilización se va a incrementar, en primer lugar, por el perfil de los usuarios, los llamados nativos digitales, cuyo modo de relación natural con las administraciones será a través de los medios digitales y en segundo lugar, por la generalización en el uso de dispositivos móviles de tercera y cuarta generación que permitirán acceder e interactuar con dichos medios digitales con una mayor facilidad.

En este contexto, es esencial reforzar la confianza de los usuarios en los sitios web de la AGE ya sea como medio de información, de participación o para la utilización de los servicios de las sedes electrónicas y es necesario también mejorar la usabilidad y la calidad de dichos sitios web, mediante el impulso de la normalización de características tales como su apariencia y sus condiciones de uso, así como mediante el cumplimiento de los requisitos normativos.

Así, la «Guía de Comunicación Digital para la Administración General del Estado» presenta un marco de criterios, recomendaciones y buenas prácticas a tener en cuenta por los Departamentos y Organismos vinculados o dependientes de la AGE, tanto al crear nuevos sitios web como al dotarlos de contenidos o evolucionar y mantener los sitios ya existentes.

La Guía también recopila la abundante normativa aplicable a los sitios web de la AGE y en particular, en materia de: imagen institucional, multilingüismo, accesibilidad o seguridad.

La presente Guía actualiza: la «Guía para la edición y publicación de las páginas web de la Administración General del Estado» de 2005 y de 2008; el «Borrador de la Guía de

páginas web de la AGE» de 2009 y la «Guía de Sedes electrónicas» de 2010, reuniendo dichos documentos en uno único y ampliándolos con indicaciones a la hora de dotar de contenidos a los sitios web o sobre la presencia de la AGE en las redes sociales, que no se contemplaban en los citados documentos.

La «Guía de Comunicación Digital para la Administración General del Estado» se divide en ocho fascículos, que pueden ser utilizados conjunta o independientemente y dos anexos técnicos.

Los fascículos se refieren a diversas materias como son: Aspectos Generales que trata de la navegación, la legibilidad, las consideraciones técnicas, los sitios para dispositivos móviles y el acceso con autenticación; Imagen Institucional que indica el uso de los logotipos del Gobierno de España en los sitios web, el uso de elementos distintivos de imagen en las redes sociales o la imagen promocional de la administración electrónica; Multilingüismo; Accesibilidad; Seguridad; Aspectos de Comunicación; Tecnologías web 2.0 (blogs, cuentas o perfiles de redes sociales), que contiene las recomendaciones sobre los contenidos y las normas de participación en las redes sociales y por último, Mejora y Mantenimiento en el que se aconseja sobre las técnicas y métricas a utilizar en los sitios web una vez puestos en marcha.

Los anexos técnicos se refieren a los Perfiles, que contiene una descripción de los recursos humanos necesarios para las distintas tareas a realizar en la puesta en marcha o mantenimiento de los sitios web de la AGE y a la Normativa que recopila la legislación ya publicada que es de aplicación en este ámbito.

La «Guía de Comunicación Digital para la Administración General del Estado» ha sido elaborada por el Ministerio de Hacienda y Administraciones Públicas, concretamente por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado para la Administración Pública, en colaboración con la Secretaría de Estado de Comunicación del Ministerio de la Presidencia.

La presente Guía ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica con la participación de todos los Departamentos Ministeriales a los que les es de aplicación.

Atendiendo a la complejidad y diversidad de aspectos que hay que tener en cuenta al elaborar y mantener los sitios web de la AGE, se considera necesaria la publicación de esta resolución de la Secretaría de Estado de Administraciones Públicas, la cual aprueba e insta a la aplicación de la «Guía de Comunicación Digital para la Administración General del Estado», que aglutina los criterios y recomendaciones y clarifica las instrucciones que deban ser observadas al respecto por los distintos departamentos y organismos de la AGE.

En consecuencia, en virtud de las competencias atribuidas por el artículo 16.1 e), f) y g) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, resuelvo:

Primero. *Aprobación y aplicación de la «Guía de Comunicación Digital para la Administración General del Estado».*

1. Se aprueba la «Guía de Comunicación Digital para la Administración General del Estado», que estará disponible en el Portal de la Administración Electrónica. (http://www.administracionelectronica.gob.es)

2. Los sitios web, elaborados por los Departamentos u Organismos Públicos vinculados o dependientes de la AGE para cualquier tipo de dispositivo, procurarán observar las recomendaciones, criterios y buenas prácticas establecidos en dicha Guía, de manera gradual en la medida en que sus circunstancias, en cuanto a recursos humanos y disponibilidad presupuestaria, lo permitan.

Segundo. *Actualización de la Guía.*

La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, oída la Comisión Permanente del Consejo Superior de Administración Electrónica llevará a cabo la actualización de la «Guía de Comunicación Digital para la Administración General del Estado» cuando lo considere necesario.

Tercero. *Difusión de la Guía.*

La presente Guía y sus futuras versiones se distribuirán a los Departamentos y Organismos a través de la Comisión Permanente del Consejo Superior de Administración Electrónica y se publicarán en el apartado de Documentación: Metodologías y Guías del Portal de la Administración Electrónica: http://www.administracionelectronica.gob.es.

Los elementos relativos a la Imagen Institucional para contribuir al cumplimiento de los criterios establecidos en esta Guía se facilitarán a los Departamentos y Organismos en el espacio: http://imagen.funciona.es/ al que se accede a través de la Red SARA.

Cuarto. *Aplicación.*

La «Guía de Comunicación Digital para la Administración General del Estado» que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Quinto. *Pérdida de efectos.*

La presente Resolución sustituye a las siguientes disposiciones, que quedan sin efecto:

– «Resolución de 9 de marzo de 2005 de la Secretaria General para la Administración Pública por la que se aprueba la Guía para la edición y publicación de páginas web en la Administración General del Estado».

– El apartado Cuarto y el Anexo II de la "Resolución de 2 de abril de 2007, de la Secretaría General para la Administración Pública (BOE de 16 de abril), por la que se modifica el Manual de Imagen Institucional de la Administración General del Estado y la Guía para la edición y publicación de páginas web en la Administración General del Estado aprobada por Resolución de 9 de marzo de 2005 de la Secretaría General para la Administración Pública."