

Incidencia del desarrollo reglamentario en la adaptación de las Administraciones Locales a la Ley 11/2007

Anexo a la Guía práctica de la Ley 11/2007,
de Acceso Electrónico de los Ciudadanos a los Servicios Públicos



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO



FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS

INCIDENCIA DEL DESARROLLO REGLAMENTARIO EN LA ADAPTACIÓN DE LAS ADMINISTRACIONES LOCALES A LA LEY 11/2007

ANEXO A LA GUÍA PRÁCTICA DE LA LEY 11/2007,
DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS
A LOS SERVICIOS PÚBLICOS



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

EDITA

FEMP

AUTORES

Dña. Virginia Moreno Bonilla
Directora de Sistemas de Información
Ayuntamiento de Leganés

D. Valentín Pérez Almarza
Director de Organización, Información y Calidad
Ayuntamiento de Leganés

DISEÑO Y MAQUETACIÓN

Pixel CPG, s.l.

IMPRESIÓN

Gráficas Varona

ISBN: 978-84-92494-17-0

Depósito Legal: S.693-2010

Edición: 2010

La edición impresa de esta publicación ha sido posible gracias al Convenio firmado entre el Ministerio de Industria, Turismo y Comercio y la FEMP dentro de las actuaciones del Plan Avanza 2.

Índice



1. Antecedentes: Guía práctica sobre la ley 11/2007	5
2. El desarrollo reglamentario de la Ley 11/2007	7
3. Resumen por temas clave	9
3.1. Sede Electrónica	9
3.2. Registro Telemático	11
3.3. Notificaciones	13
3.4. Tablón de Anuncios	16
3.5. Firma del personal al servicio de las administraciones públicas	17
3.6. Habilitación de funcionarios	18
3.7. Habilitación de Terceros	19
3.8. Gestión Documental	20
3.9. Desarrollos pendientes	29
3.10. Nuevos proyectos de Ley	31
4. Ordenanza reguladora de la administración electrónica	33
4.1. Ordenanza Tipo. Esquema guía	33
4.2. Convenios con Diputaciones. Adhesión a convenios	36
5. Liderazgo, igualdad y compromiso político	37
6. Principales problemas técnicos con plataformas comunes	39
6.1. Red SARA	39
6.2. @Firma	45
7. Búsqueda de soluciones comunes	50
7.1. CITA: Catálogo para intercambio y transferencia tecnológica.	50
8. Glosario de términos	51
9. Anexo I. Ejemplos de ordenanzas	55
9.1. Ayuntamiento de Leganés	55
9.2. Ayuntamiento de Rivas-Vaciamadrid	93
9.3. Ayuntamiento de Irún	129
10. Anexo II. Nuevas normativas	157
10.1. Real Decreto 1671/2009 de 6 de Noviembre	157
10.2. Real Decreto 4/2010 de 8 de Enero. Esquema Nacional de Interoperabilidad	189
10.3. Real Decreto 3/2010 de 8 de Enero. Esquema Nacional de Seguridad	210

Antecedentes: Guía Práctica sobre la Ley 11/2007

1.

El 23 de Junio del año 2007 se publicó en el Boletín Oficial del Estado y un día después entró en vigor la **Ley 11/2007**, de **Acceso Electrónico de los Ciudadanos a los Servicios públicos**, en adelante **LAECSP**, cuya finalidad es promover el uso de las Tecnologías de la Información y las Comunicaciones en las relaciones entre la Administración Pública y los ciudadanos y entre las diferentes Administraciones Públicas. En virtud de esta Ley, los ciudadanos podrán realizar todas sus gestiones administrativas por medios electrónicos. De esta forma, las Administraciones Públicas quedan obligadas a ofrecer sus servicios por Internet, dispositivos móviles, TDT o cualquier medio electrónico futuro.

Anteriormente a la LAECSP, la **Ley 30/1992**, de 26 de Noviembre, de **Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC)** ya recogía en algunos de sus artículos el impulso por parte de la Administración al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos al objeto de desarrollar su actividad y el ejercicio de sus competencias así como posibilitaba que los ciudadanos pudieran relacionarse con las Administraciones Públicas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos cuando esto fuera compatible con los medios técnicos de que dispusieran éstas. Las avanzadas, para el momento, pero por otra parte prudentes, previsiones legales, muy válidas en 1992, habían quedado desfasadas, ante una realidad en la 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 correspondía ya con los servicios meramente facultativos que la citada Ley permitía y estimulaba a establecer a las distintas Administraciones.

Este desarrollo de la administración electrónica era todavía insuficiente, en buena medida debido a que las previsiones indicadas en la ley eran facultativas. Es decir, dejaban en manos de las propias Administraciones determinar si los ciudadanos iban a poder de modo efectivo, o no, relacionarse con ellas por medios electrónicos, según que éstas quisieran poner en pie los instrumentos necesarios para esa comunicación. Por esta razón la ley 11/2007 pretendió dar el paso del “podrán” al “deberán” es decir, lo que en la ley 30/1992 se planteaba como algo opcional y recomendable en la ley 11/2007 pasa a ser una obligación.

En resumen, la Ley 30/1992 se limitó a abrir la posibilidad de establecer relaciones telemáticas con la Administración, pero era necesaria otra regulación que garantizara, de modo efectivo, 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 nuevas exigencias. Esta regulación común exige, reconocer el derecho de los ciudadanos –y no sólo la posibilidad- de acceder mediante comunicaciones electrónicas a la Administración.

Con la intención de facilitar en el ámbito de la Administración Local la aplicación de estas normativas y teniendo en cuenta el horizonte temporal del 1 de Enero de 2010 se elaboró desde la Comisión de Modernización y Calidad de la FEMP la “Guía práctica de aplicación de la Ley 11/2007 en la Administración Local”.

Dicho documento tenía por objeto presentar una **Guía de introducción y adaptación a la LAECSP para Administraciones locales**, realizando una descripción de los contenidos de la misma, con el objetivo de facilitar su mejor comprensión e interpretación, así como subrayar los aspectos de especial relevancia, para que cualquier Ayuntamiento o Diputación utilizando esta guía pueda, según sus características, orientar su adaptación a la Ley 11/2007 o realizar una planificación acorde a la misma.

En noviembre de 2009 apareció 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. Este real decreto pretende ser un complemento necesario en la Administración General del Estado para facilitar la efectiva realización de los derechos reconocidos en la ley.

Ya iniciado el año 2010 se han publicado dos nuevos Reales Decretos que definen los tan esperados Esquema nacional de Interoperabilidad y Esquema Nacional de Seguridad.

La incidencia de esta nueva normativa en la adaptación de las entidades locales a la Ley 11/2007 nos ha llevado, con el impulso de la Comisión de Modernización y Calidad de la FEMP a desarrollar el presente documento como anexo a la anterior guía y con el objetivo de concretar la directrices y tareas que tienen que definir y llevar a cabo los distintos Ayuntamientos y Diputaciones para poder afrontar el cumplimiento de la Ley 11/2007.

El desarrollo reglamentario de la Ley 11/2007

2.

■ ■ **Real Decreto 1671/2009 de 6 de Noviembre**

El Real Decreto desarrolla los derechos reconocidos en la Ley 11/2007, de 22 de junio en el ámbito de la Administración General del Estado.

Aunque no tiene carácter básico para las restantes administraciones, sirve de norma supletoria en tanto en cuanto no exista una normativa específica para aquellas.

El Real Decreto, se marca como objetivos, primero, 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 y 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 citada Ley, 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.

■ ■ **Real Decreto 3/2010 de 8 de Enero. Esquema Nacional de Seguridad**

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 servicio.

Este decreto es de aplicación a todas las administraciones incluidas en el ámbito de aplicación de la Ley 11/2007.

■ ■ **Real Decreto 4/2010 de 8 de Enero. Esquema Nacional de Interoperabilidad**

El Esquema Nacional de Interoperabilidad comprende los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deben 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.

Este decreto también es de aplicación a todas las administraciones incluidas en el ámbito de aplicación de la Ley 11/2007.

Las principales obligaciones que se derivan de este real decreto, son:

- 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.
- 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.
- Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes.

Resumen por temas clave

3.

Vamos a realizar a continuación un planteamiento temático de la incidencia que los tres reales decretos han tenido en el desarrollo de la Ley, haciendo un resumen de esta y resaltando las principales aportaciones de los reales decretos en cada uno de los puntos tratados. En el texto se han eliminado las referencias que podrían hacer que pareciera que su aplicación se limita a la Administración General del Estado, dado el carácter supletorio del Real Decreto 1671/2009. Aunque se ha respetado en lo posible la literalidad de las normas, se han eliminado las referencias a otras normas anteriores y al propio articulado, dado el carácter divulgativo del texto, con el fin de hacer más sencilla su comprensión.

3.1. Sede Electrónica

■ Ley 11/2007

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.

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.

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.

Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras.

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

En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones que pueden presentarse en el mismo.

■ ■ Real Decreto 1671/2009

■ *Contenido y servicios de las sedes electrónicas.*

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, 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 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.

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 de acceso.
- d. Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.
- e. Acceso al estado de tramitación del expediente.
- f. Publicación de los diarios o boletines.
- g. 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.

Los órganos titulares responsables de la sede podrán además incluir en la misma otros servicios o contenidos.

No será necesario recoger en las subsedes la información y los servicios indicados cuando ya figuren en la sede de la que aquéllas derivan.

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.

■ *Reglas especiales de responsabilidad*

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.

Observaciones

En un Ayuntamiento, la forma más adecuada para crear y regular la sede electrónica, sería la aprobación de la misma como parte de una ordenanza municipal de administración electrónica.

3.2. Registro Telemático

■ ■ **Ley 11/2007**

La Ley regula la creación de registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

Estos registros pueden admitir tanto documentos electrónicos normalizados, cumplimentados de acuerdo con formatos preestablecidos, como cualquier solicitud, escrito o comunicación dirigidos a cualquier órgano o entidad del ámbito de la administración titular del registro, pudiendo aportarse asimismo otros documentos, siempre que estos cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad.

La ley contempla la obligación de emitir automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación, incluyendo la fecha y hora de presentación y el número de entrada de registro. Los registros electrónicos también deben generar recibos acreditativos de la entrega de los documentos aportados, de forma que se garantice la integridad y el no repudio de los mismos.

En la sede electrónica de acceso al registro debe figurar la relación actualizada de las solicitudes, escritos y comunicaciones normalizadas que pueden presentarse así como, en su caso, la posibilidad de presentación de cualquier otra solicitud, escrito o comunicación.

También se especificaba en la ley que las Administraciones Públicas podrían, mediante convenios de colaboración, convenir con otras administraciones la recepción de las solicitudes, escritos y comunicaciones.

■ ■ **Real Decreto 1671/2009**

■ *Creación de los registros*

El real decreto establece los contenidos mínimos de las disposiciones de creación de los registros electrónicos:

- 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.

■ **Medios de presentación no contemplados**

Para evitar posibles vías alternativas no controladas de presentación, el real decreto determina que no tienen la condición de registro electrónico los buzones de correo electrónico corporativo asignado a los empleados públicos o a las distintas unidades y órganos, ni los dispositivos de recepción de fax, salvo aquellos supuestos expresamente previstos en el ordenamiento jurídico.

■ **Rechazo de solicitudes**

También hace una relación de las Solicitudes, escritos y comunicaciones que pueden ser rechazados en los registros electrónicos:

- 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, o cuando contenga incongruencias u omisiones que impidan su tratamiento.
- d. Que se trate de documentos que deban presentarse en registros electrónicos específicos.

En estos casos, establece la obligación de informar 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.

Si el rechazo no se ha producido automáticamente, a pesar de concurrir alguna de las circunstancias descritas, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiéndole que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia.

■ **Interrupción del servicio**

El real decreto detalla las circunstancias de interrupción del servicio:

Por el tiempo imprescindible sólo cuando concurren razones justificadas de mantenimiento técnico u operativo. La interrupción deberá anunciarse a los potenciales usuarios del registro electrónico con la antelación que 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.

■ *Emisión de justificantes*

Se desarrolla en el real decreto la emisión de justificantes que contemplaba la Ley.

El registro electrónico emitirá automáticamente por el mismo medio un recibo firmado electrónicamente, 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.

Observaciones

Aunque la ley daba la posibilidad de convenir con otras administraciones la recepción de las solicitudes, escritos y comunicaciones, el real decreto limita la recepción por la Administración del Estado a los escritos dirigidos a la propia Administración del Estado. ¿Qué lógica tiene la recepción de solicitudes, escritos y comunicaciones dirigidos a otra administración cuando el registro de esta debe encontrarse igualmente en Internet? No tiene sentido en el entorno telemático la recepción de solicitudes, escritos y comunicaciones dirigidos a una administración distinta a la receptora.

3.3. Notificaciones

■ ■ Ley 11/2007

La Ley dice que 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. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento podrán emitirse y recabarse por medios electrónicos.

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.

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, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.

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 la Ley 30/1992.

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.

■ ■ **Real Decreto 1671/2009**

■ *Práctica de la notificación*

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.

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. 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 y el real decreto.

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

■ *Formas de notificación:*

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

1. Mediante la dirección electrónica habilitada para la notificación

Serán válidos los sistemas de notificación 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.

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.

Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada será asignada de oficio y podrá tener vigencia indefinida.

■ 2. *Mediante sistemas de correo electrónico con acuse de recibo*

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.

■ 3. *Mediante comparecencia electrónica en la sede*

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.

Para que la comparecencia electrónica produzca los efectos de notificación, se requerirá que reúna las siguientes condiciones:

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.

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

4. **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.

Observaciones

Los ayuntamientos pueden utilizar sistemas externos de notificación. Pueden realizarse las notificaciones formalizando un convenio con la Sociedad Estatal Correos y Telégrafos o contratando a alguna de las empresas que ofrece estos servicios en el mercado.

Aunque, lógicamente esto supone pagar un precio por cada notificación, será con seguridad menor que el resultante de establecer y mantener un sistema de notificación propio, y en todo caso, siempre será menor que el de realizar las actuales notificaciones en papel.

3.4. Tablón de Anuncios

■ ■ Ley 11/2007

La ley dice que la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente. Permite de hecho, la eliminación del tablón de anuncios en soporte papel.

■ ■ Real Decreto 1671/2009

■ *Requisitos*

El Real Decreto establece que las notificaciones y publicaciones electrónicas cumplan 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.

Observaciones:

¿Qué sentido tiene que una administración publique en Internet las resoluciones o actos de otra, que está a su vez obligada a publicarlo en este mismo canal? Si eliminamos el tablón de anuncios en soporte papel ¿estamos obligados a publicar los edictos, requerimientos y notificaciones de otras administraciones que obligatoriamente, hasta ahora, debíamos publicar en el tablón en soporte papel?

El antiguo tablón de anuncios era un fichero de datos no estructurado. Aún así, la normativa de protección de datos nos limitaba la publicación de datos personales. El paso al entorno electrónico supone dar una disponibilidad de los datos propia de un fichero estructurado.

Sólo podremos publicar documentos que contengan datos personales cuando sean públicos, es decir cuando se publique simultáneamente en un boletín o diario oficial, o en casos específicos (por ejemplo: procesos en régimen de concurrencia cuya publicación se haya contemplado en la aprobación de sus bases).

3.5. Firma del personal al servicio de las Administraciones Públicas

■ ■ Ley 11/2007

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.

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.

Podrá utilizarse la firma electrónica basada en el Documento Nacional de Identidad.

■ ■ Real Decreto 1671/2009

■ *Tipos de firma electrónica mediante medios de autenticación personal*

- a. Firma basada en el Documento Nacional de Identidad electrónico.
- b. Firma basada en certificado de empleado público al servicio de la Administración.
- c. Sistemas de código seguro de verificación.

■ *Características de los sistemas de firma electrónica basados en certificados facilitados al personal de la Administración*

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

La firma electrónica deberá cumplir con las garantías que se establezcan en las políticas de firma que sean aplicables.

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.

Observaciones

La firma basada en certificado de empleado público al servicio de la Administración tiene la ventaja sobre la firma basada en el Documento Nacional de Identidad electrónico o sobre las firmas que pudieran basarse en otro tipo de certificados en que, al revocarse cuando el empleado cesa en su puesto de trabajo, garantiza que el documento fue firmado mientras el empleado desempeñaba su cargo. En el caso del DNI o de otros certificados, sólo se puede asegurar que fueron firmados durante la vigencia de los mismos, pero no aseguran que en firmante desempeñara el puesto en el momento de la firma.

3.6. Habilitación de funcionarios

■ ■ Ley 11/2007

■ *Identificación y autenticación de los ciudadanos por funcionario público*

La Ley dice que 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, 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.

Para la eficacia de lo dispuesto, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación prevista.

■ ■ Real Decreto 1671/2009

■ *Identificación y autenticación de los ciudadanos por funcionario público.*

Para llevar a cabo la identificación y autenticación de los ciudadanos por funcionario público 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.

Se mantendrá actualizado un registro de los funcionarios habilitados en la 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.

3.7. Habilitación de Terceros

■ ■ Ley 11/2007

La Ley contempla la posibilidad de 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.

■ ■ Real Decreto 1671/2009

El real decreto regula la habilitación contemplada en la Ley, y distingue entre representación habilitada y apoderamiento.

■ *Representación habilitada*

La habilitación requiere la firma previa de un convenio entre el Ministerio u organismo público competente y la corporación, asociación o institución interesada (colegios profesionales, asociaciones profesionales...).

Los Convenios de habilitación surten 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 deben suscribir un documento individualizado de adhesión que recoja expresamente la aceptación de su contenido íntegro.

Las personas o entidades habilitadas para la presentación electrónica de documentos en representación de terceros deben ostentar la representación necesaria para cada actuación. 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 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.

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

■ *Apoderamiento*

Se crea el registro electrónico de apoderamientos en el ámbito de la Administración del Estado. 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.

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 podrán requerir al interesado la correspondiente subsanación.

Observaciones

Parece que el real decreto abre el camino para que cada administración firme sus propios Convenios de habilitación y sus propio registro electrónico de apoderamiento.

Si existiera la posibilidad de adhesión de las restantes administraciones a los Convenios firmados por la Administración General del Estado o si se abriera el registro de apoderamientos a los otorgados ante otras administraciones, se facilitarían significativamente, en costes y tiempo, el ejercicio de la representación.

3.8. Gestión Documental

La gestión documental es el elemento clave de la administración electrónica en general y de la tramitación electrónica y la interoperabilidad en particular. Es el ámbito que la normativa desarrolla con más profundidad dedicándole una parte importante de los contenidos del Real Decreto 1671/2009 y la mayor parte del Esquema Nacional de Interoperabilidad.

■ ■ Ley 11/2007

■ *El documento electrónico*

Las Administraciones Públicas pueden emitir validamente los documentos administrativos por medios electrónicos siempre que incorporen una o varias firmas electrónicas.

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

■ *Copias electrónicas*

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, 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.

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.

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.

En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

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.

■ *El archivo electrónico de documentos*

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

Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes electrónicos, 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.

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.

■ *Expediente electrónico*

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

El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante. 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.

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.

■ ■ **Real Decreto 1671/2009**

■ *El documento electrónico*

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.

Los documentos administrativos electrónicos deberán, además de cumplir las anteriores condiciones, haber sido expedidos y firmados electrónicamente, y ajustarse a los requisitos de validez previstos en la Ley 30/1992.

Se asociará a los documentos electrónicos la información relativa a la firma del documento así como la referencia temporal de los mismos.

■ **Los metadatos**

El decreto introduce en la normativa el concepto de metadato, concepto básico para la implantación de la administración electrónica.

Se entiende como metadato, 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.

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.

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.

Independientemente de los metadatos mínimos obligatorios, 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 la prohibición de modificación.

■ **Copias electrónicas de los documentos electrónicos**

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.

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.

Se podrán generar copias electrónicas auténticas a partir de otras copias electrónicas auténticas siempre que se observen estos requisitos.

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.

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, será considerado también copia electrónica auténtica de documentos electrónicos presentados conforme a sistemas normalizados o formularios.

■ ***Copias electrónicas de documentos en soporte no electrónico***

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.

Cuando sean realizadas por la Administración, las imágenes electrónicas tendrán la naturaleza de copias electrónicas auténticas, 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.
- 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.

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.

■ ***Copias en papel de los documentos públicos administrativos electrónicos realizadas por la propia Administración***

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.

■ ***Destrucción de documentos en soporte no electrónico***

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 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.
- 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.

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.

■ ***Referencia temporal de los documentos administrativos electrónicos***

Se asociarán a los documentos administrativos electrónicos 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» entendiéndose 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», entendiéndose 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.

■ *Imágenes electrónicas aportadas por los ciudadanos*

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.

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.

La presentación documental que realicen los interesados en cualquiera de los lugares de presentación establecidos, podrá acompañarse de soportes conteniendo documentos electrónicos.

■ *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.

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.

■ *Obtención de copias electrónicas a efectos de compulsas*

Cuando los interesados deseen aportar 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 presentados.

Estas copias digitalizadas serán firmadas electrónicamente y tendrán el carácter de copia compulsada o cotejada, sin que en ningún caso se acredite la autenticidad del documento original.

■ *Archivo electrónico de documentos*

Se deberán conservar en soporte electrónico todos los documentos electrónicos que formen parte de un expediente administrativo, así como aquellos otros que, tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.

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.

■ *Conservación de documentos electrónicos*

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 documentos electrónicos.

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.

■ *Formación del expediente electrónico*

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

El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado electrónicamente.

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.

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

Observaciones:

El real decreto determina que 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.

■ ■ **Real Decreto 4/2010 de 8 de Enero. Esquema Nacional de Interoperabilidad**

■ *Recuperación y conservación del documento electrónico*

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.

■ *Repositorios electrónicos*

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.

■ *Seguridad*

Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimiento 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.

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.

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.

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.

■ **Formatos de los documentos**

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.

Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el 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.

■ **Digitalización de documentos en soporte papel**

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.
- b. Nivel de resolución.
- c. Garantía de imagen fiel e íntegra.
- d. Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

3.9. Desarrollos pendientes

El Esquema Nacional de Interoperabilidad prevé un desarrollo por medio de normas técnicas de interoperabilidad (de obligado cumplimiento) e instrumentos para la Interoperabilidad.

■ Normas técnicas de interoperabilidad

- 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 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.

■ *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.

Observaciones:

Para cumplir la normativa es necesario implantar un sistema de gestión documental que dé soporte al repositorio único de documentación que deberá soportar la integración de imágenes y metadatos y las funcionalidades descritas.

La gestión de los metadatos, es algo que sólo puede realizarse si se automatiza su generación de forma que los metadatos se cumplimenten automáticamente al realizar las tareas administrativas de registro, tramitación, notificación, etc. Si se pretendieran cumplimentar de forma independiente a las aplicaciones de gestión, se generaría una carga de trabajo adicional difícilmente asumible. Esto implica la necesidad de integrar las aplicaciones de gestión de la organización con el gestor documental.

Si una administración pretende poner en marcha de forma inmediata un sistema integrado de tramitación electrónica, digitalizando la documentación recibida en papel, dándole valor pleno mediante la compulsión electrónica e integrándola en un repositorio único de documentación, incorporando sistemas de firma electrónica, etc. se arriesgará a que cuando se aprueben las normas técnicas de interoperabilidad, los sistemas implantados no sean coherentes con las mismas, y se pierda parte o todo el trabajo realizado.

Dada la lentitud del desarrollo de la Ley 11 (más de un año y medio desde su publicación hasta la publicación de los esquemas de Interoperabilidad y Seguridad) y considerando las previsiones que el propio Esquema Nacional de Interoperabilidad establece, podría esperarse, sin un excesivo pesimismo, que la normativa completa no esté disponible antes de otro año y medio, con la correspondiente inseguridad para las administraciones que intenten avanzar en la aplicación práctica de la Ley 11.

3.10. Nuevos proyectos de Ley

Para dar cumplimiento a la directiva europea de servicios, se tramitan en la actualidad dos proyectos de Ley conocidos popularmente como Ley paraguas y Ley ómnibus. Estos proyectos inciden en la administración electrónica en cuanto dictan las normas de funcionamiento de la llamada Ventanilla única.

■ ■ Ley Paraguas

A los efectos de acreditar el cumplimiento de los requisitos exigidos para el acceso y ejercicio de una actividad de servicios, las Administraciones Públicas aceptarán los documentos procedentes de otro Estado miembro de los que se desprenda que se cumplen tales requisitos. En el caso de documentos emitidos por una autoridad competente, no se exigirá la presentación de documentos originales o copias compulsadas ni traducciones juradas, salvo en los casos previstos por la normativa comunitaria, o justificados por motivos de orden público y de seguridad pública.

Todos los procedimientos y trámites que supeditan el acceso y ejercicio a una actividad de servicios se podrán realizar electrónicamente y a distancia salvo que se trate de la inspección del lugar o del equipo que se utiliza en la prestación del servicio.

Los prestadores de servicios podrán acceder, electrónicamente y a distancia a través de una ventanilla única, tanto a la información sobre los procedimientos necesarios para el acceso y ejercicio de una actividad de servicios, como a la realización de los trámites preceptivos para ello, incluyendo las declaraciones, notificaciones o solicitudes necesarias para obtener una autorización, así como las solicitudes de inscripción en registros, listas oficiales, asociaciones y colegios profesionales.

Las Administraciones Públicas promoverán que los prestadores de servicios puedan a través de la ventanilla única:

- a. Obtener toda la información y formularios necesarios para el acceso y ejercicio de su actividad.
- b. Presentar toda la documentación y solicitudes necesarias.
- c. Conocer el estado de tramitación de los procedimientos en que tenga la condición de interesado, y recibir la correspondiente notificación de los actos de trámite preceptivos y la resolución de los mismos por el órgano administrativo competente.

■ *Garantías de información a través de la ventanilla única*

Los prestadores y los destinatarios podrán obtener, a través de la ventanilla única y por medios electrónicos, la siguiente información, que deberá ser clara e inequívoca:

- a. Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los trámites necesarios para acceder a las actividades de servicios y su ejercicio, así como los datos de las autoridades competentes que permitan ponerse en contacto directamente con ellas.
- b. Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a los prestadores y a los servicios.

- c. Las vías de reclamación y los recursos que podrán interponerse en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores.
- d. Los datos de las asociaciones sectoriales de prestadores de servicios y u las organizaciones de consumidores que presten asistencia a los prestadores y destinatarios de los servicios.

Las Administraciones Públicas adoptarán medidas para fomentar que en la ventanilla única pueda accederse a la información contemplada en el presente artículo en otras lenguas comunitarias.

■ ■ Ley Ómnibus

“Cuando se trate de procedimientos y trámites relativos a una actividad de servicios y a su ejercicio incluida en el ámbito de aplicación de la Ley.../... sobre el libre acceso a las actividades de servicios y su ejercicio, los prestadores podrán realizarlos, por medio de una ventanilla única, por vía electrónica y a distancia, salvo que se trate de la inspección del lugar o del equipo que se utiliza en la prestación del servicio.

Asimismo, las Entidades locales promoverán que los prestadores de servicios puedan a través de la ventanilla única obtener toda la información y formularios necesarios para el acceso a una actividad y su ejercicio, y conocer las resoluciones y resto de comunicaciones de las autoridades competentes en relación con sus solicitudes.»

Las Administraciones Públicas tendrán permanentemente publicados y actualizados modelos de declaración responsable y de comunicación previa que en todo caso se podrán presentar por vía electrónica.»

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:

- 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 de las asociaciones sectoriales de prestadores de servicios y las organizaciones de consumidores que presten asistencia a los prestadores y destinatarios de los servicios.
- 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.»

Ordenanza reguladora de la administración electrónica

4.

4.1. Ordenanza Tipo. Esquema guía

La incorporación a la administración electrónica requiere que cada Administración determine las condiciones e instrumentos de creación de las sedes electrónicas. También es necesario regular los distintos elementos que intervienen en el acceso electrónico de los ciudadanos y en las comunicaciones electrónicas dirigidas a estos: registros, notificaciones y tablones de anuncios electrónicos, habilitación de funcionarios, representación de los interesados, etc.

El marco más adecuado es la aprobación de un instrumento normativo u Ordenanza que además de dar cabida a las necesidades manifestadas, sirva para divulgar entre los ciudadanos los derechos y obligaciones que les otorga la Ley 11/2007 y promueva la utilización de los medios electrónicos puestos a su disposición.

En este capítulo se propone una estructura estándar de ordenanza con el fin de facilitar su elaboración.

Esta estructura estándar se ha dividido en capítulos y los aspectos cuyo tratamiento se propone son los mínimos que deben tenerse en cuenta para asegurar la regulación de los aspectos básicos de la Ley 11/2007.

■ Estructura tipo:

EXPOSICIÓN DE MOTIVOS

CAPÍTULO PRIMERO.

Disposiciones generales.

Artículo 1. Objeto.

Artículo 2. Definiciones.

Artículo 3. Ámbito de aplicación.

CAPÍTULO SEGUNDO.

Principios generales.

Artículo 4. Principios organizativos de la administración electrónica.

Artículo 5. Difusión de la información.

Artículo 6. Procedimiento administrativo electrónico.

Artículo 7. Principios de cooperación con otras Administraciones Públicas.

CAPÍTULO TERCERO.

Derechos y deberes de los ciudadanos en la relación con la administración electrónica.

Artículo 8. Derechos de la Ciudadanía.

Artículo 9. Deberes de la Ciudadanía.

Artículo 10. Cumplimiento de derechos y deberes.

CAPÍTULO CUARTO.

La Sede Electrónica.

Artículo 11. Características de la Sede Electrónica.

Artículo 12. Identificación de interesados y autenticación de su actuación.

Artículo 13. Identificación y autenticación de los Órganos administrativos.

Artículo 14. Identificación y autenticación de las sedes.

CAPÍTULO QUINTO.

La difusión de la información administrativa por medios electrónicos.

Artículo 15. Acceso a la información.

Artículo 16. Información sobre la organización y servicios de interés general.

Artículo 17. Información administrativa

Artículo 18. Tablón de Edictos Electrónico.

Artículo 19. Publicación oficial.

CAPÍTULO SEXTO.

Oficina Virtual, Registro, comunicaciones y notificaciones electrónicas.

Artículo 20. Oficina Virtual.

Artículo 21. Registro Electrónico de entrada y salida de documentos.

Artículo 22. Escritos y documentos susceptibles de registro de entrada.

Artículo 23. Cómputo de plazos en Registro Electrónico.

Artículo 24. Régimen de funcionamiento del Registro Electrónico.

Artículo 25. Autenticidad, integridad, confiabilidad, disponibilidad y conservación del contenido de los asientos electrónicos.

Artículo 26. Las comunicaciones electrónicas.

Artículo 27. Las notificaciones electrónicas.

CAPÍTULO SÉPTIMO.

Los documentos y archivos electrónicos.

Artículo 28. Documento Administrativo electrónico.

Artículo 29. Copias Electrónicas.

Artículo 30. Compulsa electrónica de documentos en soporte papel.

Artículo 31. Archivo Electrónico.

Artículo 32. Expediente electrónico.

CAPÍTULO OCTAVO.

Gestión electrónica de los procedimientos. Disposiciones comunes.

Artículo 33. Trámites y procedimientos a los que es aplicable la tramitación electrónica.

Artículo 34. Mecanismo de incorporación de trámites y procedimientos a la tramitación por vía electrónica.

CAPÍTULO NOVENO.

Utilización de medios electrónicos en la tramitación del procedimiento.

Artículo 35. Iniciación del procedimiento administrativo.

Artículo 36. Representación.

Artículo 37. Tramitación del procedimiento administrativo.

Artículo 38. Continuación del procedimiento administrativo electrónico por medios tradicionales.

Artículo 39. Acceso de los interesados a la información sobre el estado de La Tramitación del procedimiento.

Artículo 40. Terminación de los procedimientos por medios electrónicos.

Artículo 41. Actuación administrativa automatizada.

CAPÍTULO DÉCIMO.

Servicio Telemático de Pago.

Artículo 42. Servicio Telemático de Pagos.

DISPOSICIONES TRANSITORIAS.

DISPOSICIONES FINALES.

ANEXO I. Trámites y gestiones municipales disponibles en la sede electrónica

Opcional, ya que quedará contemplado en la definición oficial de la Sede Electrónica de cada Ayuntamiento.

En resumen:

- *En el Capítulo Primero, se presentan el objetivo y el ámbito de aplicación*
- *En el Capítulo Segundo, los principios generales definidores de este nuevo concepto de Atención a la Ciudadanía*
- *En el Capítulo Tercero, se establecen los derechos y deberes de los ciudadanos*
- *En el Capítulo Cuarto, las características de la Sede Electrónica*

- *En el Capítulo Quinto, la difusión de la información por medios electrónicos*
- *En el Capítulo Sexto, la oficina virtual, los registros y notificaciones electrónica*
- *En el Capítulo Séptimo, los documentos y archivos electrónicos*
- *En el Capítulo Octavo, la gestión electrónica de los procedimientos*
- *En el Capítulo Noveno, la utilización de medios electrónicos y la tramitación electrónica del procedimiento*
- *Y finalmente en el Capítulo Décimo, el servicio telemático de pago.*

4.2. Convenios con Diputaciones. Adhesión a convenios.

Una solución posible para los municipios a los que la falta de recursos les dificulte la aprobación de su propia Ordenanza reguladora, podría ser su adhesión a la Ordenanza aprobada por la correspondiente Diputación, Cabildo o Comunidad Autónoma mediante la firma de un convenio.

Algunas Diputaciones ya ofrecen a sus municipios la posibilidad de establecer este tipo de convenio.

Liderazgo, igualdad y compromiso político

5.

El objetivo de este capítulo es intentar reflexionar sobre conceptos que a veces consideramos obvios y dejamos pasar sin darles la importancia necesaria, y que a la hora de poder dar cumplimiento a determinadas normativas, en este caso el cumplimiento de la Ley 11/2007, son más importantes para el éxito del proyecto que el tipo de tecnología que apliquemos.

Vamos a utilizar, por adecuarse totalmente a lo que queremos expresar, una intervención realizada por Fran Belver, Teniente de Alcalde de Gobernación del Ayuntamiento de L'Hospitalet de Llobregat, en una jornada de formación continua celebrada en su Ayuntamiento a finales de 2009.

La titulaba: **“LIDERAZGO POLÍTICO EN LA APLICACIÓN DE LA LEY 11/2007”** y su contenido era el siguiente:

“El líder es alguien que tiene una postura activa ante la realidad, mediante la cual quiere cambiar algo de su entorno.

¿Ese liderazgo, esa postura ante la realidad (cambio tecnológico, sociedad del conocimiento, qué significa para las administraciones en particular y para los ciudadanos en general? Los líderes deben ser motivadores, educadores, modelos a imitar, portavoces y animadores. ¿Cómo se transfieren por tanto esas características, del líder anónimo a los líderes políticos y cómo se aplican en el municipio? Descubriendo los puntos débiles y fuertes de nuestro entorno fijando metas y trabajando para alcanzarlas. Asumiendo las responsabilidades y siendo conscientes de las consecuencias. Convirtiendo cada situación en una experiencia útil.

El **liderazgo** en el proceso de aplicación de la Ley 11/2007 se basa en **la garantía de aplicar diferentes valores que mejoren y desarrollen nuestro estado de bienestar facilitando así una mayor calidad de vida de nuestros vecinos y vecinas.**

Los valores que quiero destacar y que creo, pueden influir de igual manera, tanto en los ciudadanos como en la administración, permitiendo de esta manera mejorar el sistema de relaciones son:

La **proximidad** como una oportunidad para poner en valor los servicios públicos = Entendida como una forma de comunicación cercana a los ciudadanos, que garantice además la bidireccionalidad de la comunicación, ya no es la Admón. la única que comunica.

La **modernización** entendida como el proceso de adopción y adaptación de las TIC para facilitar el necesario cambio cultural no sólo en la sociedad sino también en el interior de las organizaciones/administraciones, que garantice el éxito y la eficiencia de la ley.

La **equidad** entendida como principio fundamental para generar y garantizar la igualdad de oportunidades entre todos y todas.

Los valores por tanto de la Proximidad, modernización y equidad nos han de servir para definir el papel de los políticos en la aplicación y desarrollo de la Ley 11/2007.

La Ley no es un fin. La ley es por tanto el medio para conseguir una administración próxima y facilitadora de la modernización y la equidad. Compromiso de los políticos con la sociedad para garantizar la proximidad a través de la Administración Pública. Facilitando el acceso a los servicios y los recursos conseguiremos una sociedad más cercana.

Compromiso de los políticos con la sociedad para garantizar la modernización a través de la Administración Pública. Si somos capaces de crear una administración inteligente (entendiendo el concepto inteligente cómo la capacidad de adaptación a los cambios), conseguiremos una sociedad más moderna.

Compromiso de los políticos con la sociedad para garantizar la equidad a través de la Administración Pública, si universalizamos los servicios y los recursos conseguiremos tener una sociedad donde sus individuos en su conjunto cuentan con las mismas oportunidades.

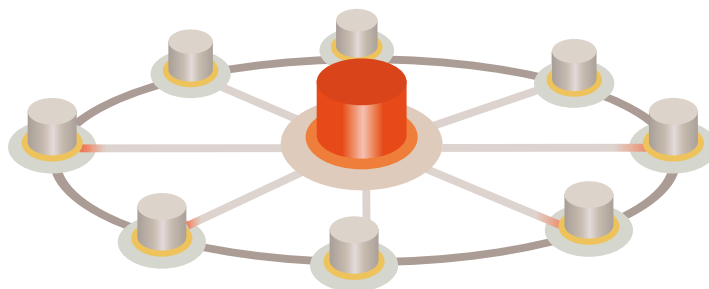
Hemos de ser capaces por tanto de transmitir a la ciudadanía que sólo el esfuerzo de todos y todas facilitará que nuestra sociedad se convierta en una sociedad moderna, avanzada y viva, capaz de asimilar los grandes cambios y los grandes retos a los cuales nos enfrentamos de forma individual y colectiva. Para ello será necesario además que las redes sociales, de relación y de comunicación que hoy inundan nuestro entorno no consigan deshumanizar nuestra sociedad y nuestros vínculos.”

Principales problemas técnicos con plataformas comunes

6.

6.1. Red SARA

El artículo 43 de la Ley 11/2007 establece la obligación de crear una red de comunicaciones que interconecte las Administraciones Públicas españolas, entre si y con otras redes de las Instituciones Europeas y de otros Estados miembros, para el intercambio de información y servicios. La Red SARA permite la interconexión de las administraciones públicas, facilitando el intercambio de información y servicios. A través de la Red SARA los Ministerios, las Comunidades Autónomas, los Entes Locales y otros organismos públicos pueden interconectar sus redes de una manera fiable, segura, capaz y flexible.



■ ■ Características de la red SARA:

- **Fiabilidad:** La red SARA está diseñada con tecnología de última generación VPLS (Virtual Private LAN Services) que la dota de gran capacidad de transmisión de datos. Además, su diseño y tecnología le permiten ofrecer una muy alta disponibilidad para garantizar en todo momento la continuidad del servicio, lo cual se complementa con la existencia de un Centro de Soporte 24 x 7 con unos exigentes acuerdos de nivel de servicio (SLA's).
- **Seguridad:** SARA implementa medidas de seguridad entre las que destaca el establecimiento de VPNs. Es una red extremadamente segura en la que todo el tráfico circula cifrado por la Troncal. De esta manera queda asegurada la confidencialidad de la información que viaja a través de la red SARA.
- **Capacidad:** Esta red cuenta con un ancho de banda de 1 Gbps en Ministerios y CPD's (10 veces más que su predecesora), y 100 Mbps en cada Comunidad Autónoma (50 veces más caudal) lo que permite asegurar la capacidad para absorber las exigentes demandas tanto de las aplicaciones existentes como de los nuevos servicios de administración electrónica.

- **Calidad de Servicio (QoS):** La tecnología VPLS utilizada en el diseño de la red SARA permite dotarla de mecanismos de calidad de servicio para tratar cada dato transmitido de acuerdo a su naturaleza (voz, video, datos), lo cual establece un nuevo abanico de servicios multimedia a incorporar.
- **Punto-multipunto:** La red SARA está diseñada con un modelo de conexión punto-multipunto (“todos con todos”) mediante el cual no existe un nodo central en el que convergen todas las conexiones y por tanto se eliminan posibles puntos únicos de fallo. Esta topología se complementa perfectamente con la arquitectura de seguridad existente, en la cual los mecanismos de seguridad están distribuidos en cada nodo, si bien la política es homogénea y con gestión centralizada.
- **Flexibilidad:** En el diseño de la red SARA se ha tenido en cuenta la posibilidad de que esta red pueda evolucionar y crecer a medida que lo hagan las necesidades de la administración.

■ *Organismo*

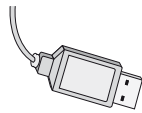
Ministerio de Presidencia. Dirección General para el Impulso de la Administración Electrónica.

■ *Servicios vía SARA*

- Verificación de los datos de identidad y residencia.
- Plataforma de validación de firma electrónica.
- Notificación fehaciente electrónica.
- Pasarela de pago.
- Registro electrónico común.
- Consultas del estado de expedientes.
- Catálogos de procedimientos de las AAPP.
- Simulación de dichos procedimientos.
- Servicios de nueva creación.
- Videoconferencia.
- Voz IP.
- Entornos de trabajo colaborativo.
- Servicios de la Comisión Europea y de otros Estados miembros.

■ **Contactos y Soporte**

secretaria.redsara@mpr.e



<http://cst.actualize.es/inquiere/anonymos21.asp>

A screenshot of a web browser window. The address bar shows 'inc/default_new.asp'. The browser has a menu bar with 'Archivo', 'Edición', 'Ver', 'Favoritos', 'Herramientas', and 'Ayuda'. Below the menu bar is a toolbar with icons for home, search, and print. The main content area features a banner for 'Ayuda On-Line' from the 'Comunidad de Madrid' with a large red and white logo. Below the banner is a 'Política de privacidad' link. The main form contains the text: 'Contactaremos con usted lo antes posible, deje aquí su petición. Horario: 24 horas al día, los 365 días del año.' The form fields include: '*Su e-mail:' (text input), '*Mensaje:' (text area), 'Nombre:' (text input), 'Apellidos:' (text input), 'Compañía:' (text input), and 'Teléfono:' (text input). A vertical scrollbar is on the right side of the form.

■ ■ Requisitos de uso

Por el momento, no requiere convenio con el Ministerio de Presidencia, si bien el Ministerio de Presidencia ha firmado convenios con casi todas las Comunidades Autónomas.

Los Ayuntamientos se conectan a través del nodo de su Comunidad Autónoma, aunque para ello se puede firmar un anexo de adhesión al convenio.

Si no se tuviese acceso a esta red, se puede habilitar temporalmente un acceso a pre-producción en algunos de los servicios, como es el caso de @firma (únicamente mientras se gestiona la integración a la red SARA).

El acceso a la red SARA debe realizarse a través de la Comunidad Autónoma, en caso de desconocer a quién dirigirse se solicitaría apoyo al contacto y soporte arriba mencionados.

■ ■ Cómo se gestiona el acceso a la Red SARA

Nota: se toma como ejemplo el procedimiento establecido en la Comunidad de Madrid

En el caso de la Comunidad de Madrid el proceso sería el siguiente:

■ A) Ayuntamientos a la Red SARA SSL VPN

1. Enviar una solicitud de Acceso SARA, designando un Coordinador Técnico del Ayuntamiento, junto con la petición de alta al sistema de dicho coordinador, a:

Dirección General de Calidad de los Servicios y Atención al Ciudadano
C/ Gran Vía, 18 2ª planta, 28013 – Madrid.

El Coordinador Técnico del Ayuntamiento será el interlocutor técnico con ICM (Informática y Comunicaciones de la Comunidad de Madrid) para:

- Autorizaciones de acceso de los usuarios del Ayuntamiento.
- Reporte de incidencias o problemas del Servicio.
- Complimentar el Modelo de solicitud: Ficha de solicitud de alta del Coordinador Técnico // www.madrid.org/ayuntamientos_ae

2. Autorización de usuarios de acceso del Ayuntamiento.

El Coordinador Técnico del ayuntamiento, mediante esta ficha, mantendrá actualizada la relación de usuarios del Ayuntamiento que estén capacitados para el acceso a SARA, a través de este Servicio. Ficha de solicitud de alta de empleados del Ayuntamiento // www.madrid.org/ayuntamientos_ae

Una vez cumplimentada la ficha y firmada por el Coordinador Técnico, se deberá escanear el documento -si no se ha utilizado firma electrónica para la firma del mismo- y se enviará por correo electrónico a la dirección ICM_DASC_PRESIDENCIA@madrid.org

De esta forma se tiene acceso al servicio Ayuntamientos a la Red SARA SSL VPN a través de un usuario y un password.

■ B) Conexión Site to Site. Acceso entre sistemas del Ayuntamiento y Comunidad de Madrid

Las conexiones "Site to Site" se establecen técnicamente entre el Coordinador Técnico del Ayuntamiento y el personal Técnico de la Dirección de Comunicaciones de ICM. El establecimiento del contacto inicial se realizará a través de la Dirección General de Calidad de los Servicios y Atención al Ciudadano y para su inicio es requisito el cumplimentar y remitir el siguiente cuestionario:

Red SARA en las Administraciones Locales

(Ficha para la creación de la red privada virtual con la CM a través de Internet)



Administración Local			
Ubicación			
Contacto			
e-mail			Teléfono
Subred GTA cliente (cumplimentar por la CM)	Servicios básicos en Red SARA: <input type="checkbox"/> DNS <input type="checkbox"/> Proxy <input type="checkbox"/> MTA <input type="checkbox"/> NTP <input type="checkbox"/> SOCKS (no operativo aún) <input type="checkbox"/> UDDI (no operativo aún)	Servicios no básicos en Red SARA: <input type="checkbox"/> Aplicaciones Cliente/Servidor <input type="checkbox"/> Otras (Especificar requisitos)	

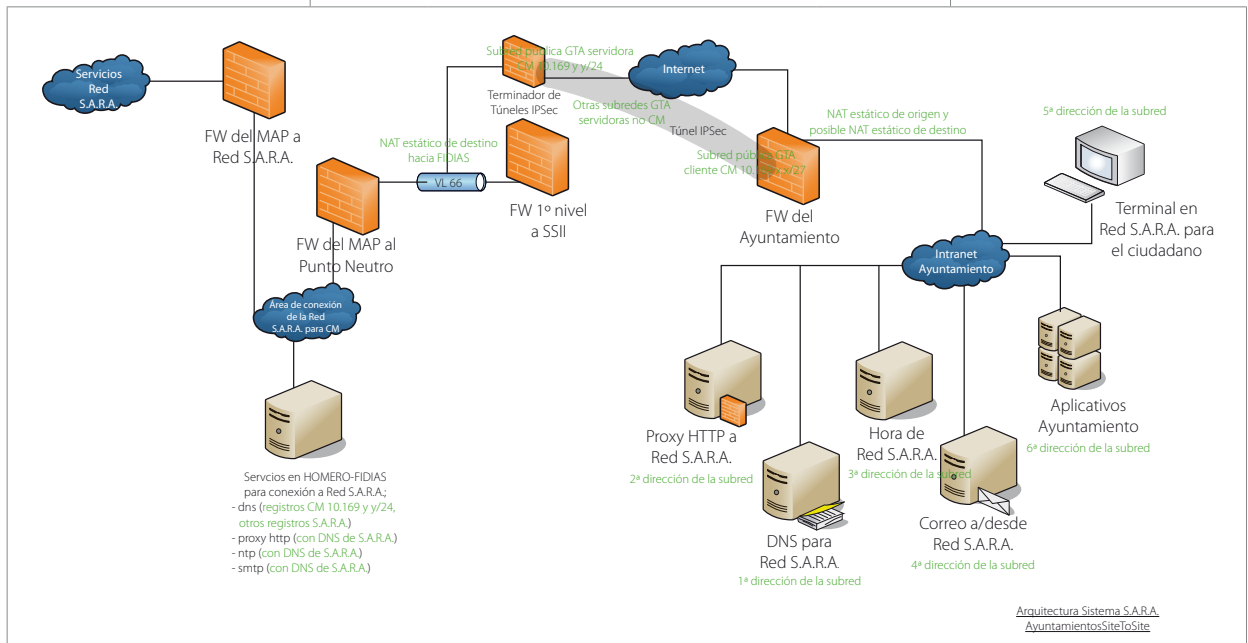
DESCRIPCIÓN GENERAL

En la Red SARA conviven todos aquellos servicios que conforman la Intranet Administrativa. En concreto el MAP delega en cada Comunidad Autónoma unos servicios generales que pueden servir para alcanzar servicios de la Intranet Administrativa de una forma transparente o con menor o ninguna participación de los intermediarios ("Servicios básicos en Red SARA"). Por otro lado, el ofrecimiento de "Servicios no básicos" en Red Sara obliga a los intermediarios a un encaminamiento directo entre cliente y servicio con las consiguientes acciones técnicas. Pero en ambos casos el diálogo en Red SARA se debe realizar usando el direccionamiento ip GTA que el MAP asigna a las administraciones públicas. Es por ello que a la administración local se le asignará un direccionamiento GTA cliente a usar dentro de la red privada virtual establecida con la CM y que el servicio básico de DNS sólo ofrece registros GTA.

La red privada virtual con la CM se establece a través de Internet teniendo como punto de establecimiento el nombre público de Internet:

accesovpn.madrid.org

Administración Local	
Ubicación	
Contacto	
e-mail	Teléfono



REQUISITOS DE LA VPN A TRAVÉS DE INTERNET

El establecimiento de la red privada virtual se basa en IPSec cuyos parámetros de configuración en el extremo de CM son:

- Encriptación: 3DES
- Firma: Hash SHA-1
- Autenticación: certificados con verificación local (en CM) de CRL

El procedimiento a seguir en la emisión de certificados será el siguiente:

- El Ayuntamiento generará en su equipo, extremo de la red privada virtual, la solicitud de firma de su certificado (CSR).
- El Ayuntamiento enviará por correo electrónico a <¿cuenta correo a usar?> el CSR generado en el paso anterior con los siguientes parámetros:
 - O = "Nombre del Ayuntamiento"
 - C = es (indica el código del país)
- La CM, a la recepción del correo, firmará el CSR y anexará además el certificado raíz de la autoridad de certificación para su instalación en el equipo del Ayuntamiento.

DESCRIPCIÓN DE LOS SERVICIOS NO BÁSICOS EN RED SARA

Posteriormente, es necesario remitir a la Comunidad Autónoma (en este caso, ICM) los siguientes datos:

- CSR con la solicitud del certificado en formato PKCS10 con los siguientes parámetros:
- CN=Ayuntamiento de XXXXXXXXX, OU=Comunidad Autónoma , C=ES
- La IP pública del equipo desde el que se establece la conexión al servidor de túneles.

Y por parte del departamento de mantenimiento y seguridad de la Comunidad (ICM): El direccionamiento asignado con el que la entidad debe presentarse 10.xxx.xx.x/xx, así como los parámetros de configuración para la VPN:

Fase 1: Cifrado 3DES, Hash MD5. Autenticación con certificado, sin verificación CRL. Grupo DH 2.

Fase 2: Cifrado 3DES, Hash MD5. , indicando la IP pública del firewall con la que la entidad debe terminar xxx.xx.xxx.xxx, así como los rangos de la red SARA a los que tendrá acceso dicha entidad y que en el caso de querer acceso a servicios tales como @firma, deberá notificar a soporte técnico de dicha herramienta de validación y firma electrónica.

■ ■ Dificultades más comunes

En el caso de la configuración Site to Site a través de la red SARA, y en concreto en el caso de la Comunidad de Madrid, la dificultad estriba en la interlocución y acceso a los responsables de ICM. No se dispone de teléfono de soporte ni correo genérico de acceso público.

Otro de los motivos que dificulta el acceso a la red SARA es la necesidad de cumplimiento de todos los protocolos de actuación en los que implica el contacto con el nivel de soporte inicial que es el propio ministerio de presidencia, para después acceder al interlocutor correspondiente de cada comunidad autónoma y por último en este caso, contactar con el organismo encargado de la gestión del Servicio (ICM).

En el caso de las administraciones locales, la dificultad de acceso estriba en la necesidad de disponer de routers de acceso con la tecnología y sistemas operativos que soporte los protocolos de cifrado y seguridad exigidos para la interconexión a la red SARA.

Como solución se propone que en la ficha explicativa de los servicios y requisitos de acceso a la red sara se publiquen las tablas de contactos y accesos de cada comunidad autónoma, disponiendo de una dirección de correo y teléfono de soporte.

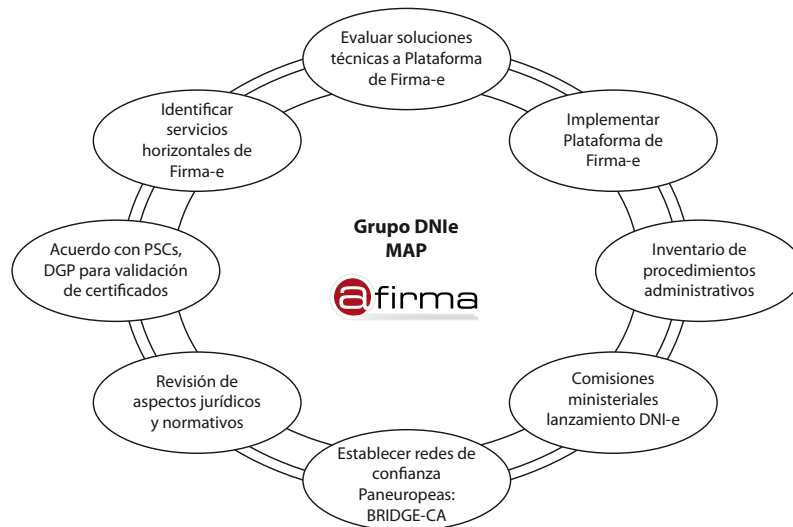
Para terminar diremos que la red SARA es un instrumento fundamental para seguir avanzando en el desarrollo de la administración electrónica, lo que en definitiva supone mejorar el servicio prestado a los ciudadanos.

6.2. @Firma

Es la solución tecnológica en la que se basa la implementación de la Plataforma de validación y firma electrónica del Ministerio de Presidencia. La versión actual de @firma es la 5.0 y constituye una evolución de la versión 4.0 a partir de la aportación de múltiples Organismos Públicos cooperantes.

Es un producto robusto e integral, desarrollado inicialmente por la Junta de Andalucía, cedido al resto de las Administraciones Públicas con el objeto de fomentar y extender el desarrollo de la Administración Electrónica y la Sociedad de la Información.

Es una solución basada en software libre, estándares abiertos y en java: servidores Web Apache, JBOSS, Sistema Operativo Solaris/Linux, AXIS, etc. Y se puede acceder sin coste alguno ni compromiso con diferentes CAs, a unos 60 certificados de 12 entidades diferentes, entre los que está el eDNI.



■ ■ Servicios:

- **Validación de certificados** X.509 según la RFC 3280, de las Autoridades de Certificación incluidas en la plataforma.
- **Funcionalidades de firma:** La plataforma permite varias modalidades de firma.
- **Validación** de la firma de un elemento firmado.
- Proporciona un **cliente de firma** que permite a los ciudadanos que accedan a los servicios de Administración Electrónica, firmar electrónicamente los documentos.
- **Sellado de Tiempo** (TSA) según el estándar RFC 3161 para certificar temporalmente todas las operaciones de validación y firma que se realizan a través de la plataforma.
- **Gestión y administración** de los Prestadores de Servicios de Certificación adheridos. Todas las operaciones realizadas en la plataforma son registradas para la auditoría y trazabilidad del sistema.

La plataforma @firma es una solución de referencia para cumplir con las medidas de identificación y autenticación descritas en el Capítulo II de la Ley 11/2007. Para acceder a los servicios indicados es necesario disponer de accesibilidad a la Plataforma @firma desde los sistemas de información del Organismo en cuestión a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que ofrece servicios de intranet entre las Administraciones Públicas.

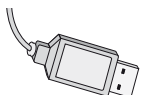
■ ■ Requisitos de uso

Para acceder a los servicios es necesario disponer de accesibilidad a la Plataforma desde los sistemas de información del Organismo en cuestión, a través de la red SARA (Sistema de Aplicaciones y Redes para las Administraciones), que ofrece servicios de intranet entre las Administraciones Públicas. Estos sistemas que soportan los servicios de administración electrónica disponibles para los ciudadanos y empresas, accederán a la Plataforma a través de servicios web implementados en tecnología Microsoft® o Java.

Si no se posee un convenio o acuerdo con el Ministerio de Presidencia o con la Comunidad Autónoma de acceso e integración a la Red Sara, es necesario remitir una carta de solicitud de acceso al Director General para el Impulso a la Administración Electrónica para regularizar este aspecto, y asumir que se permite el acceso al entorno de producción de @firma.

Es necesario comprometerse a informar de los servicios que se tuvieran preparados para admitir el DNI-e, al MPA y se publicaría en la web del DNI electrónico (www.dnieelectronico.es).

■ ■ Contactos y soporte



Centro de soporte @firma del Ministerio de Presidencia//Soporte.afirma5@map.es //

Telf. 902 934 405

■ ■ Pasos a seguir

1. El Organismo debe ponerse en contacto con el servicio de soporte (CAU) de @firma, indicando el Organismo (Ministerio, Comunidad Autónoma o Entidad Local) que desea integrarse en el servicio, así como los datos de contacto del mismo:

eMail:soporte.afirma5@map.es

teléfono: 902 93 44 05

2. El servicio de Soporte (CAU) se pondrá en contacto con dicho Organismo para informar de los prerequisites que son necesarios para iniciar la integración.

Para ello es necesario:

- a. Conocer si el Organismo tiene convenio con la FNMT (para poder validar sus certificados).
 - b. Trasladar al Organismo el compromiso de informar al Ministerio de Presidencia de los servicios que utilicen la plataforma para admitir el DNIe, para publicarlo en la web del DNI electrónico.
 - c. Informar al Organismo que los servicios se ofrecen a través de la red SARA, y que durante las pruebas se pueden hacer pruebas controladas en un entorno de preproducción habilitado al efecto desde Internet.
3. Una vez informados los prerequisites, habiendo respondido el Organismo, el servicio de Soporte (CAU) le proporciona al mismo la documentación de bienvenida, que se compone de:
 - a. ACL (formulario para el control de acceso).
 - b. Documentación
 - Pasos iniciales para la integración con @firma.
 - Servicios de @firma.
 - Manual del Integrador del Cliente de Firma @firma.
 - Manual de Programación de web service de @firma.

4. El Organismo debe devolver el ACL debidamente cumplimentado al servicio de Soporte (CAU) para finalizar el proceso de integración.

Ejemplo de ACL. Elegir en primera instancia si la conexión es a través de OCSPResponder (Online Certificate Status Protocol (OCSP)) es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). o Web Services

DATOS A RELLENAR POR SISTEMAS	
IP ORIGEN	IP ACTUAL
(si es un rango, indicar la máscara)	
RESPONSABLES DE SISTEMAS	
Nombre y Apellidos	
Teléfono	
Email	
DATOS A RELLENAR POR EL ORGANISMO	
ENTORNO (Marcar con una X)	
REPRODUCCIÓN	
PRODUCCIÓN	
CERTIFICADOS ADMITIDOS	
Tipos de certificados que se van a utilizar (por Autoridad de Certificación y tipo de persona física, persona jurídica, componente, ...)	
¿Disponen de convenio en vigor con la FNMT-RCM para la prestación de servicios de certificación?	
Indique fecha de caducidad del convenio:	
APLICACIÓN 1 (que va a usar el servicio)	
Nombre de la aplicación	
Descripción de la aplicación	
Unidad Organizativa	
<u>Responsable</u>	
Nombre y Apellidos	
Teléfono	
Email	
Lista de los servicios telemáticos que se soportarán con la aplicación URL donde se ubican los servicios telemáticos	
...	
APLICACIÓN N (que va a usar el servicio)	
Nombre de la aplicación	
Descripción de la aplicación	
Unidad Organizativa	
<u>Responsable</u>	
Nombre y Apellidos	
Teléfono	
Email	
Lista de los servicios telemáticos que se soportarán con la aplicación URL donde se ubican los servicios telemáticos	
Formato de la Firma de Respuesta	
Método de Autorización	

XAdEST (Firma XML avanzada con sellado temporal)	<input checked="" type="checkbox"/>
XMLDSignature (Firma XML Básica)	
XAdESBES (Firma XML Avanzada)	
XAdEST (Firma XML avanzada con sellado temporal)	<input checked="" type="checkbox"/>
Sin método de autorización	
<input type="checkbox"/>	
Sin método de autorización	
Usuario y Password	
Certificado	

5. En el caso de una conexión haciendo uso del certificado de componente, es necesario remitir al servicio de @firma el certificado con la clave pública que se va a utilizar en las conexiones con @firma, así como el formato de exportación del certificado.
6. Para el acceso a pre-producción es necesario indicar la IP de salida del organismo que desea conectarse a este entorno.
7. El servicio de Soporte (CAU) informará debidamente de los parámetros de conexión con los servicios: URL, identificador de aplicaciones,...

■ **Las URL de los servicios son las siguientes:**

- Desarrollo (SARA): <http://des-afirma.redinteradministrativa.es/afirmaws/services/>
- Producción (SARA) <http://afirma.redinteradministrativa.es/afirmaws/services/>
- Pre-producción Desarrollo (Internet): <http://217.15.39.2/afirmaws/services/>

En este último caso, siempre con el permiso de la Coordinación del proyecto del MPR.

■ ■ **Dificultades más comunes**

La necesidad de integrarse en la red Sara para hacer uso del servicio en entorno de desarrollo o explotación.

Sugerencia: En el caso de que el acceso al entorno de desarrollo no requiriera el cumplimiento de todas las especificaciones técnicas, podrían realizarse pruebas en un entorno similar al de producción, con el consiguiente ahorro de tiempo que conlleva la tramitación administrativa de solicitud y acceso a la red Sara.

7. *Búsqueda de Soluciones Comunes*

7.1. CITA: Catálogo para intercambio y transferencia tecnológica

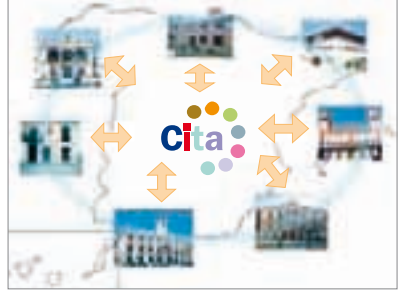
Plataforma Avanza Local Soluciones	
Aplicaciones informáticas que facilitan la gestión interna de las entidades, el desarrollo de la Administración electrónica y la prestación de Servicios Públicos Digitales	
SIGEM	Para la gestión administrativa de la entidad
Local web	Aplicación para la creación y gestión de portales municipales
Local GIS	Sistema de Información Geográfico
Avanza Catastro	Módulo para el tratamiento on-line de la información urbana y catastral
Avanza Local Padrón	Sistema Integrado de Gestión de Padrón y Censo de habitantes
e-fácil	Incorpora la factura electrónica (formato facturae). Incluye módulo (CIRCE local)
CITA	Cátalogo para el intercambio y transferencia de aplicaciones
Rendición de cuentas	Para la optimización del proceso de rendición de cuentas al Tribunal de Cuentas por las EE.LL.

CITA

Cooperación entre administraciones para el impulso de la administración electrónica:

Fomenta la **coordinación, la transferencia y el intercambio de herramientas** entre entidades de todo el territorio nacional a través del MITYC

A) Visitantes que podrán conocer las aplicaciones seleccionadas y las EELL que las desarrollan.



B) Socios cuyo compromiso supone intercambiar y transferir conocimiento.

<http://www.planavanza.es/AvanzaLocal>

Glosario de términos



■ ■ **Identidad Electrónica**

Contempla la Identificación del Ciudadano y la Identificación de los trabajadores públicos: posibilidad de utilizar cualquier tipo de identificación electrónica admitida legalmente y se admitirán certificados electrónicos reconocidos emitidos por otras administraciones públicas.

■ ■ **Sede Electrónica**

Dirección electrónica disponible para la Ciudadanía para realizar tramites y procedimientos administrativos, y consultar cualquier tipo de información en poder el Ayuntamiento.

La titularidad, la gestión y la administración de esa dirección corresponden al Ayuntamiento.

■ ■ **Registro telemático**

Gestiona y mecaniza la información relativa a las comunicaciones entre el Ayuntamiento y el exterior, dejando constancia de cada una de ellas. El escaneado agiliza la aportación controlada de documentos durante el proceso.

■ ■ **Gestor de Expedientes**

Permite la gestión y seguimiento transversal de los expedientes, garantizando criterios de tramitación homogénea e información integrada en toda la organización.

■ ■ **Repositorio único de documentos**

Cualquier documento generado o capturado por un usuario de gestión del Ayuntamiento se almacena automáticamente en el repositorio documental.

■ ■ **Archivo electrónico**

Garantiza a largo plazo la integridad, autenticidad, disponibilidad, conservación y legibilidad de los documentos mediante reglas de clasificación y calendarios de conservación.

■ ■ 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.

■ ■ Notificaciones telemáticas seguras

El sistema de notificación acreditará la fecha y hora en que se pone a disposición del interesado la notificación, así como el momento en que se produce el acceso a su contenido.

■ ■ SNTS (Servicio de Notificaciones Telemáticas Seguras)

Servicio que el Ministerio de las Administraciones Públicas en colaboración con Correos pone a disposición de los ciudadanos.

Para recibir notificaciones a través del SNTS ello será necesario que el usuario realice las siguientes actuaciones:

- optar por este sistema de notificación marcando la casilla correspondientes al iniciar el procedimiento
- crear una Dirección Electrónica Unida (DEU) dentro de la plataforma del MAP y Correos
- suscribirse al procedimiento dentro de la plataforma del MAP y Correos

■ ■ Catálogo de procedimientos y servicios

Dentro del proyecto de Administración Electrónica se contempla la elaboración del “Catálogo de Procedimientos y Servicios de un Ayuntamiento”

El catálogo es un instrumento de referencia que recopila, describe, clasifica, y categoriza todos los procedimientos y servicios existentes y en vigor en una organización. Deberá incluir todos los procedimientos y servicios que actualmente se gestionan. Esta recopilación constituirá un inventario actualizado que permitirá planificar de manera ordenada la incorporación de todos los procedimientos y servicios a una plataforma de tramitación electrónica en la organización.

■ ■ 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.

■ ■ Canales

Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc).

■ ■ Certificado electrónico

Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, «Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad».

■ ■ Certificado electrónico reconocido

Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica: «Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten».

■ ■ Ciudadano

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

■ ■ Dirección electrónica

Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

■ ■ 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.

■ ■ 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 (art. 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica).

■ ■ Firma electrónica avanzada

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 (art. 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica).

■ ■ Firma electrónica reconocida

Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma (art. 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica).

■ ■ 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.

■ ■ 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.

■ ■ Prestador de actividad de servicio

Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

■ ■ Prestador de servicios de certificación

Es aquella persona física o jurídica que, cumpliendo los requisitos que determina la legislación establecida sobre firma electrónica, está capacitado para emitir certificados electrónicos. En la legislación española a los “prestadores de servicios de certificación” se les denomina también “terceras partes de confianza”. Tiene mucho sentido esta segunda denominación, pues lo que hacen es actuar entre emisor y receptor como tercera parte que garantiza que cada cual es quien dice ser sin posibilidad de error. Es importante que esta tercera parte de confianza nos ofrezca las suficientes garantías.

■ ■ Punto de acceso electrónico

Conjunto de páginas web agrupadas en un dominio de Internet cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios dirigidos a resolver necesidades específicas de un grupo de personas o el acceso a la información y servicios de una institución pública.

■ ■ Sistema de firma electrónica

Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

■ ■ Sellado de tiempo

Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

■ ■ Tablón de Anuncios

Debe contemplar todos los mecanismos de seguridad que implica el paso de una gestión manual a otra automática, por lo que el nuevo sistema deberá contemplar los elementos de seguridad de acceso a la información, control de integridad, firma electrónica de documentos, certificación informatizada de las fechas de publicación y despublicación del contenido, validación del original electrónico, generación del edicto de publicación, etc.

Debe ofrecer información y contenidos de libre acceso para todos los ciudadanos.

ANEXO I. Ejemplos de ordenanzas

9.

■ ■ Ejemplos prácticos de Ordenanzas aprobadas en Ayuntamientos

En este capítulo y a modo de ayuda para la elaboración y desarrollo de la Ordenanza Reguladora de la Administración Electrónica en el ámbito de la Administración Local se procede a poner 3 ejemplos de Ordenanzas de Administración Electrónica de tres Ayuntamientos distintos en población, territorio y composición del Gobierno Municipal.

También se adjuntan direcciones (url's) de otras administraciones locales para poder consultar otras ordenanzas de administración electrónica que sin duda aportan valor.

- Ayuntamiento de Leganés
- Ayuntamiento de Rivas-Vaciamadrid
- Ayuntamiento de Irún
- Otras Ordenanzas

9.1. Ayuntamiento de Leganés

■ *Ordenanza Reguladora de la Administración Electrónica del Ayuntamiento de Leganés*

ÍNDICE

EXPOSICIÓN DE MOTIVOS

CAPÍTULO 1º. Disposiciones generales

Artículo 1. Objeto.

Artículo 2. Definiciones.

Artículo 3. Ámbito de aplicación.

CAPÍTULO 2º. Principios generales

Artículo 4. Principios organizativos de la administración electrónica.

Artículo 5. Difusión de la información.

Artículo 6. Procedimiento administrativo electrónico.

Artículo 7. Principios de cooperación con otras Administraciones Públicas.

CAPÍTULO 3º. Derechos y deberes de los ciudadanos en la relación con la administración electrónica

Artículo 8. Derechos de la Ciudadanía.

Artículo 9. Deberes de la Ciudadanía.

Artículo 10. Cumplimiento de derechos y deberes.

CAPÍTULO 4º. La Sede Electrónica

Artículo 11. Características de la Sede Electrónica.

Artículo 12. Identificación de interesados y autenticación de su actuación.

Artículo 13. Identificación y autenticación de los Órganos administrativos.

Artículo 14. Identificación y autenticación de las sedes.

CAPÍTULO 5º. La difusión de la información administrativa por medios electrónicos

Artículo 15. Acceso a la información.

Artículo 16. Información sobre la organización y servicios de interés general.

Artículo 17. Información administrativa.

Artículo 18. Tablón de Edictos Electrónico.

Artículo 19. Publicación oficial.

CAPÍTULO 6º. Oficina Virtual, Registro, comunicaciones y notificaciones electrónicas

Artículo 20. Oficina Virtual.

Artículo 21. Registro Electrónico de entrada y salida de documentos.

Artículo 22. Escritos y documentos susceptibles de registro de entrada.

Artículo 23. Cómputo de plazos en Registro Electrónico.

Artículo 24. Régimen de funcionamiento del Registro Electrónico.

Artículo 25. Autenticidad, integridad, confiabilidad, disponibilidad y conservación del contenido de los asientos electrónicos.

Artículo 26. Las comunicaciones electrónicas.

Artículo 27. Las notificaciones electrónicas.

CAPÍTULO 7º. Los documentos y archivos electrónicos

Artículo 28. Documento Administrativo electrónico.

Artículo 29. Copias Electrónicas.

Artículo 30. Compulsas electrónicas de documentos en soporte papel.

Artículo 31. Archivo Electrónico.

Artículo 32. Expediente electrónico.

CAPÍTULO 8º. Gestión electrónica de los procedimientos. Disposiciones comunes

Artículo 33. Trámites y procedimientos a los que es aplicable la tramitación electrónica.

Artículo 34. Mecanismo de incorporación de trámites y procedimientos a la tramitación por vía electrónica.

CAPÍTULO 9º. Utilización de medios electrónicos en la tramitación del procedimiento

Artículo 35. Iniciación del procedimiento administrativo.

Artículo 36. Representación.

Artículo 37. Tramitación del procedimiento administrativo.

Artículo 38. Continuación del procedimiento administrativo electrónico por medios tradicionales.

Artículo 39. Acceso de los interesados a la información sobre el estado de La Tramitación del procedimiento.

Artículo 40. Terminación de los procedimientos por medios electrónicos.

Artículo 41. Actuación administrativa automatizada.

CAPÍTULO 10º. Servicio Telemático de Pago

Artículo 42. Servicio Telemático de Pagos.

DISPOSICIONES TRANSITORIAS

DISPOSICIONES FINALES

ANEXO I. Definiciones

ANEXO II. Trámites y gestiones municipales disponibles en la sede electrónica

■ *Exposición de motivos*

El desarrollo de las tecnologías de la información y las telecomunicaciones están produciendo cambios acelerados en todos los órdenes de la vida, tanto en lo personal como en lo social y empresarial. De forma significativa están transformándose las formas de hacer y relacionarse en todas las organizaciones, sean estas públicas o privadas. La implantación y utilización intensiva de las tecnologías de la información y de las comunicaciones, está influyendo fuertemente en la necesidad de redefinir las tareas y gestión de la administración pública.

Nos encontramos, por tanto, ante la “sociedad de la información y el conocimiento”, con profundos y constantes cambios inducidos por la incorporación de las tecnologías de la información y las comunicaciones en la vida cotidiana de nuestros ciudadanos, en su entorno social y laboral, en la actividad de las empresas e Instituciones, y por tanto en las relaciones humanas, sociales y económicas.

Uno de los ámbitos en que se están experimentando mayores transformaciones es en lo relativo a las relaciones entre los ciudadanos y las Administraciones Públicas. El Ayuntamiento de Leganés está comprometido con estos nuevos retos con el objetivo de impulsar la sociedad de la información y el conocimiento y especialmente, crear una

administración más abierta y asequible. Es intención del Ayuntamiento de Leganés actuar como agente dinamizador de la utilización de las tecnologías entre los ciudadanos y dentro de la propia administración, aprovechando todo el potencial que tienen para mejorar los servicios públicos y su relación con los ciudadanos.

El Ayuntamiento de Leganés, en ejercicio de su potestad autoorganizativa, dicta esta Ordenanza con el objeto de regular la utilización de las TIC en las relaciones jurídico-administrativas entre los ciudadanos y el Ayuntamiento.

Es necesario un instrumento normativo que determine los derechos y los deberes de los ciudadanos en este ámbito, que regule las condiciones, las garantías y los efectos jurídicos de la utilización de los medios electrónicos en las relaciones con los ciudadanos y que establezca los principios generales de actuación en esta materia, en especial en el proceso de incorporación a la administración electrónica de los trámites y los procedimientos administrativos, siempre en la línea de las propuestas de la Comisión Europea y de la OCDE, apostando por el concepto de “Administración Electrónica” entendida como la aplicación de las Tecnologías de la Información y Comunicación (TIC) en toda nuestra actuación municipal y la realización de numerosos cambios organizativos en nuestras estructuras, para mejorar los servicios públicos y el acceso a ellos por parte de los ciudadanos y de las empresas de nuestro Municipio.

Este instrumento normativo a implementar, debe dar plena seguridad jurídica a todas las partes implicadas, así como agilidad y eficacia a los servicios municipales que presta el Ayuntamiento, facilitar nuevos canales de acceso y formas de prestar los servicios a los ciudadanos sin limitaciones horarias y que reduzca o elimine sus desplazamientos.

El 24 de junio de 2007 entró en vigor la Ley 11/2007, de 22 de junio de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Dicha Ley presenta como gran novedad el reconocimiento del 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 atención al público, en la actividad administrativa en los organismos públicos, la responsabilidad de la Sede Electrónica en las diferentes administraciones, el intercambio de información entre las Administraciones Públicas y establece un marco jurídico para la Ciudadanía y las administraciones.

El compromiso del Gobierno Municipal es ofrecer a los ciudadanos un servicio público moderno, eficaz y eficiente que satisfaga plenamente sus necesidades, estableciendo todos los medios posibles para facilitar a los ciudadanos un acceso a nuestro Ayuntamiento, de manera rápida, segura y transparente.

La Ordenanza se estructura por capítulos; *en el Capítulo Primero, se presentan el objetivo y el ámbito de aplicación, en el Capítulo Segundo, los principios generales definidores de este nuevo concepto de Atención a la Ciudadanía, en el Capítulo Tercero, se establecen los derechos y deberes de los ciudadanos, en el Capítulo Cuarto, las características de la Sede Electrónica, en el Capítulo Quinto, la difusión de la información por medios electrónicos, en el Capítulo Sexto, la oficina virtual, los registros y notificaciones electrónica, en el Capítulo Séptimo, los documentos y archivos electrónicos, en el Capítulo Octavo, la gestión electrónica de los procedimientos, en el Capítulo Noveno, la utilización de medios electrónicos y la tramitación electrónica del procedimiento y finalmente en el Capítulo Décimo, el servicio telemático de pago.*

■ Capítulo 1º. *Objetivos y ámbito de aplicación*

■ ■ Artículo 1. Objeto

1. La presente Ordenanza se dicta en virtud del derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, que se consagra en la Ley 11/2007 de 22 de junio y establece la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones de los ciudadanos con las Administraciones Públicas, así como en las relaciones entre las Administraciones Públicas, con el fin de hacer posible la consecución más eficaz de los principios de transparencia administrativa, proximidad y servicio a la Ciudadanía que se derivan del artículo 103 de la Constitución, garantizando: los derechos de los ciudadanos, un tratamiento común y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.
2. Como consecuencia de lo anterior, esta **Ordenanza tiene por objeto:**
 - a. Establecer los derechos y los deberes que deben regir las relaciones que se establezcan por medios electrónicos entre la Ciudadanía y el Ayuntamiento.
 - b. Fijar los principios generales para el impulso y desarrollo de la administración electrónica en el Ayuntamiento de Leganés, regular las condiciones y los efectos jurídicos del uso de los medios electrónicos en la actividad administrativa.
 - c. Establecer los principios reguladores que han de regir la incorporación de los trámites de los procedimientos administrativos y de la utilización de canales de prestación de servicios por vía electrónica.
 - d. 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.
 - e. Promover la proximidad con la Ciudadanía y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.
 - f. Contribuir a la mejora del funcionamiento interno del Ayuntamiento de Leganés, incrementando la eficacia mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.
 - g. Simplificar los procedimientos administrativos, proporcionando, con las debidas garantías legales, oportunidades de participación y transparencia.
 - h. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.
 - i. Establecer las condiciones necesarias para la interoperabilidad de la sede electrónica del Ayuntamiento de Leganés con el resto de las sedes electrónicas de las Administraciones Públicas.

■ ■ Artículo 2. Definiciones

A efectos de la presente Ordenanza, los términos que en ella se emplean tendrán el sentido que se establece en el Anexo I, bajo la rúbrica de Definiciones.

■ ■ Artículo 3. **Ámbito de aplicación**

1. La presente ordenanza será de aplicación a:
 - a. Las Unidades Administrativas y de Atención a la Ciudadanía del Ayuntamiento.
 - b. Los organismos de derecho público pertenecientes o vinculados al Ayuntamiento.
 - c. Las sociedades y entidades concesionarias de servicios públicos municipales, cuando así lo disponga el título de concesión o lo aprueben sus órganos de gobierno, en sus relaciones con el Ayuntamiento de Leganés y con los ciudadanos, en el marco de la prestación de servicios públicos municipales y en el ejercicio de potestades administrativas de su competencia.
 - d. A la Ciudadanía, entendiéndolo como tal a las personas físicas y jurídicas, cuando utilicen medios electrónicos en sus relaciones con el Ayuntamiento y con el resto de las entidades referidas en los apartados anteriores.
 - e. A las relaciones por medios electrónicos del Ayuntamiento con otras Administraciones Públicas.
2. Esta ordenanza se aplicará a las actuaciones que se enumeran a continuación:
 - a. Las relaciones con la Ciudadanía que tengan carácter jurídico administrativo.
 - b. La consulta por parte de los ciudadanos de la información pública administrativa y de los datos administrativos que obren en poder del Ayuntamiento de Leganés.
 - c. La realización de los trámites y procedimientos administrativos incorporados a la tramitación electrónica, de conformidad con lo previsto en esta Ordenanza.
 - d. El tratamiento de la información obtenida por el Ayuntamiento de Leganés en el ejercicio de sus potestades.
 - e. A la utilización de los canales de prestación de servicios establecidos por el Ayuntamiento de Leganés de acuerdo con lo dispuesto en la presente ordenanza.

La presente Ordenanza no será de aplicación a las actividades que las Unidades del Ayuntamiento desarrollen en régimen de derecho privado.

■ **Capítulo 2º. Principios generales**

■ ■ Artículo 4. **Principios organizativos de la administración electrónica**

La utilización de las tecnologías de la información, en la actuación del Ayuntamiento, y la referida al impulso de la administración electrónica, 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:

1. Servicio al ciudadano

Se impulsará la incorporación de información, trámites y procedimientos sobre los servicios en la Sede Electrónica para posibilitar la consecución más eficaz de los principios constitucionales de transparencia administrativa, proximidad y servicio a la Ciudadanía, así como la mejora continua en la consecución del interés general.

De acuerdo al Reglamento Orgánico Municipal, el Ayuntamiento de Leganés impulsará la utilización interactiva de las tecnologías de la Información y de la comunicación para facilitar la participación y la comunicación con la Ciudadanía.

2. Simplificación administrativa

El proceso de incorporación de los medios electrónicos al procedimiento administrativo debe conllevar el análisis del proceso mismo, la reconducción a categorías generales, la implantación de determinados automatismos electrónicos, en su caso, y la eliminación de trámites o actuaciones no relevantes, de conformidad con la normativa de aplicación.

El Ayuntamiento aprovechará la eficiencia que reporta la utilización de las técnicas de los sistemas de información con el objetivo de alcanzar una simplificación e integración de los procesos, procedimientos y trámites administrativos.

3. Impulso de los medios electrónicos

Como entidad pública, el Ayuntamiento de Leganés impulsará de forma preferente el uso de los medios electrónicos en el conjunto de sus actividades y, en especial, en las relaciones con los ciudadanos, por lo que deberá aplicar los medios personales y materiales pertinentes y adoptar las medidas necesarias para su efectividad.

El Ayuntamiento podrá establecer incentivos para fomentar la utilización de los medios electrónicos entre la Ciudadanía.

4. Neutralidad tecnológica

El Ayuntamiento de Leganés garantizará la realización de las actuaciones reguladas en esta Ordenanza con independencia de los instrumentos tecnológicos utilizados en su sede electrónica, de manera que sean la misma evolución tecnológica y la adopción de las tecnologías dentro de la sociedad las que determinen la utilización de los medios tecnológicos que, en cada momento, sean más convenientes.

5. Accesibilidad e interoperabilidad

El Ayuntamiento de Leganés garantizará la adopción de los estándares de interoperabilidad y accesibilidad, respetando los criterios de seguridad, adecuación técnica y economía de medios, para que los sistemas de información utilizados por ella sean compatibles con los usados por los ciudadanos, empresas y otras administraciones.

El acceso a la Sede Electrónica estará disponible las 24 horas del día los 365 días de año.

6. Protección de la confidencialidad e integridad de los datos

El Ayuntamiento de Leganés, en el impulso de la administración electrónica, garantizará la protección de la confidencialidad y seguridad de los datos según las leyes: Ley 15/1999, Ley 11/2007 y BOE 19/01/2008.

Los datos personales de la Ciudadanía serán tratados y protegidos de forma confidencial.

Todos los datos relacionados con la actuación del Ayuntamiento estarán protegidos con sistemas de seguridad reconocidos con el fin de mantener su integridad.

7. Publicidad y transparencia

El Ayuntamiento facilitará la máxima difusión, publicidad y transparencia de la información que conste en sus archivos y de las actuaciones administrativas, de conformidad con el resto del ordenamiento jurídico y con los principios establecidos en esta ordenanza.

8. Eficacia, eficiencia y economía

La implantación de los medios electrónicos en el Ayuntamiento de Leganés estará presidida por los principios de eficacia, eficiencia y economía. En particular, se realizará según los siguientes criterios:

- a. El grado de utilización por parte de la Ciudadanía de los servicios municipales afectados.
- b. El impacto en los colectivos de población a los cuales se dirige las actuaciones.
- c. Las mejoras alcanzables en la prestación del servicio.
- d. La integración de los sistemas de atención al ciudadano con el resto de la organización y con los sistemas de información municipales.
- e. El nivel de esfuerzo técnico, organizativo y económico requerido.
- f. La madurez y disponibilidad de las tecnologías.
- g. La reducción de los plazos y tiempos de respuesta.

9. Cooperación con la sociedad civil

Con el objetivo de mejorar el servicio a la Ciudadanía, el Ayuntamiento de Leganés podrá establecer convenios, acuerdos y contratos con los colegios profesionales, asociaciones y otras entidades, para facilitar la relación de sus asociados y clientes con el Ayuntamiento.

10. Participación de la Ciudadanía

El Ayuntamiento de Leganés promoverá el uso de los medios electrónicos en el ejercicio de los derechos de participación, en especial el derecho de petición, los derechos de audiencia e información pública, la iniciativa ciudadana, las consultas y la presentación de sugerencias y reclamaciones. Asimismo, el Ayuntamiento promoverá el debate público y la expresión de ideas y opiniones, a través de diferentes tipos de instrumentos propios de los medios electrónicos, considerando en todo caso los principios de buena fe y de utilización responsable.

11. Responsabilidad Ciudadana

El Ayuntamiento de Leganés no será responsable en ningún caso de las opiniones que puedan expresar los ciudadanos cuando participen en foros de opinión, participación interactiva u otros instrumentos de participación ciudadana, por medio de la página Web de su Sede Electrónica.

12. Proporcionalidad de los controles de acceso

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.

■ ■ Artículo 5. Difusión de la información

La difusión por medios electrónicos de la información administrativa y de interés general se llevará a cabo de conformidad con los siguientes principios:

1. Disponibilidad y calidad de la información

- a. La información administrativa y de interés general estará disponible en la Sede Electrónica las 24 horas del día los 365 días del año, con calidad, garantizado a compresión de su contenido, siguiendo criterios y estándares europeos e internacionales.
- b. Los ciudadanos con discapacidad o algún tipo de diversidad funcional, tendrán los medios necesarios para acceder a la información de la Sede Electrónica, conforme a las limitaciones presupuestarias del Ayuntamiento.
- c. La disponibilidad de la información en formato electrónico no debe sustituir en ningún caso la atención personalizada que presta el Ayuntamiento de forma presencial en sus dependencias municipales o mediante la atención telefónica.
- d. La información de tipo general será de libre acceso para todos los ciudadanos.

2. Integridad y exactitud de la información publicada

El Ayuntamiento de Leganés garantizará la veracidad y autenticidad de la información a través medios electrónicos.

Los documentos electrónicos contendrán el contenido exacto y fiel al equivalente en soporte papel o en el soporte en que se haya emitido el documento original.

3. Actualización de información administrativa

Los diferentes órganos del Ayuntamiento de Leganés mantendrán actualizada la información administrativa que sea accesible a través de canales electrónicos.

La información administrativa y las publicaciones electrónicas, contendrán las fechas de actuación y el órgano u unidad responsable.

■ ■ Artículo 6. Procedimiento administrativo electrónico

Los trámites administrativos solicitados por los ciudadanos a través de medios electrónicos deberán estar regidos conformados por los siguientes principios generales:

1. No discriminación por razón del uso de medios electrónicos

Cuando un ciudadano utilice un medio diferente al medio electrónico, no podrá sufrir ningún tipo de restricción o discriminación al realizar gestiones administrativas o solicitar información general sobre los servicios que presta el Ayuntamiento.

El Ayuntamiento podrá establecer medidas dirigidas para incentivar la utilización de los medios electrónico por parte de los ciudadanos.

2. Información sobre la gestión de los procedimientos administrativos

Los ciudadanos tendrán derecho a conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, y como mínimo la fase en la que se encuentra el procedimiento y el órgano o unidad responsable de su tramitación mediante el acceso a la Sede Electrónica del Ayuntamiento.

3. Continuidad de procedimientos administrativos

Un procedimiento iniciado por un medio o canal se podrá continuar por otro diferente, siempre y cuando se pueda asegurar la integridad y seguridad jurídica del conjunto del procedimiento y si los recursos asociados a la tramitación lo permiten.

■ ■ Artículo 7. Principio de cooperación con otras Administraciones Públicas.

La cooperación con otras Administraciones Públicas en el marco de la Administración Municipal del Ayuntamiento de Leganés estará conformada por los siguientes principios generales:

1. Cooperación con otras Administraciones Públicas

El Ayuntamiento de Leganés impulsará la firma de convenios con el resto de las Administraciones Públicas, para hacer posibles y aplicables las previsiones incluidas en esta Ordenanza y dar cumplimiento a las leyes Ley 11/2007 y Ley 30/1992.

2. Acceso y disponibilidad limitada

- a. El Ayuntamiento de Leganés facilitará el acceso a su Sede Electrónica a las demás Administraciones Públicas con el fin de obtener los datos en soporte electrónico que tenga sobre los ciudadanos.
- b. El Ayuntamiento de Leganés conjuntamente con las otras administraciones especificarán las condiciones, los protocolos, los criterios funcionales y técnicos que se requerirán necesarios para acceder y obtener datos entre las administraciones, garantizando la seguridad e integridad en cada una de las Sedes Electrónicas.
- c. El suministro de datos a otras administraciones se limitará estrictamente a lo establecido en las leyes Ley 30/1992 y Ley 11/2007 u otras leyes que así lo establezcan.
- d. La solicitud de información referida a datos personales de un ciudadano, deberá ir acompañada con una autorización o consentimiento del ciudadano respectivo, tal como lo establece la Ley 15/1999.

■ ■ Capítulo 3º. *Derechos y deberes de los ciudadanos en la relación con la administración electrónica*

■ ■ Artículo 8. Derechos de la Ciudadanía.

En el marco del acceso y la utilización de la Administración Electrónica Municipal, los ciudadanos tienen los siguientes derechos:

1. Acceso a la sede electrónica

- a. Derecho a relacionarse con la Administración Municipal de Leganés a través de medios electrónicos para el ejercicio de los derechos previstos en el Art. 35 de la Ley 30/1992 de 26 noviembre.

- b. Elegir, entre aquéllos canales que en cada momento se encuentren disponibles, para relacionarse con el Ayuntamiento.
- c. Derecho a elegir la plataforma tecnológica para acceder a la Sede Electrónica y relacionarse con el Ayuntamiento de Leganés dentro de los estándares existentes en el mercado.
- d. Derecho a la calidad de los servicios públicos prestados por medios electrónicos.
- e. Derecho a utilizar los sistemas de firma electrónica del DNI-e.
- f. Derecho a utilizar los sistemas de firma electrónica avanzada reconocidas por la Administración General del Estado, según lo establecido en la Ley 59/2003.
- g. Derecho a la igualdad de todos los ciudadanos en el acceso electrónico a los servicios de atención al ciudadano de este Ayuntamiento.

2. Realizar trámites

- a. Formular solicitudes y alegaciones sobre los servicios al ciudadano que presta el Ayuntamiento de Leganés.
- b. Manifiestar consentimientos, entablar pretensiones y oponerse a las resoluciones y actos administrativos, en los procedimientos de tramitación electrónica que estén publicados en la Sede Electrónica.
- c. Derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas, para realizar trámites en la sede electrónica, según lo establece el Artículo 6.2.b de la Ley 11/2007.
- d. En los casos de solicitud de datos o documentos por otra Administración Pública, la Sede Electrónica conservará la documentación acreditativa del consentimiento expreso del ciudadano.
- e. Efectuar pagos por medio de transacciones bancarias electrónicas y obtener el respectivo comprobante.
- f. Derecho a ser representado por una persona física o jurídica.
- g. Derecho de los representantes de los ciudadanos para actuar ante el Ayuntamiento en todas aquellas actividades que el ciudadano le ha especificado en su autorización.

3. Realizar consultas

- a. Derecho a obtener información del estado de los trámites realizado mediante la sede electrónica.
- b. Derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de los procedimientos en los que tenga la condición de interesado.
- c. Derecho a que el Ayuntamiento conserve en formato electrónico los documentos electrónicos que formen parte del expediente de los trámites solicitados por la Ciudadanía.
- d. Derecho a la garantía de la seguridad y confidencialidad de los datos que figuren en las bases de datos del Ayuntamiento de Leganés.
- e. Obtener información sobre los trámites necesarios para solicitar los servicios administrativos de Ayuntamiento.
- f. Obtener información a través de la Sede Electrónica de las autoridades competentes en las materias relacionadas con las actividades de servicios al ciudadano.

4. Participación

Derecho de los ciudadanos a participar en la mejora de la gestión municipal a través de medios electrónicos, con la expresión de su opinión y expectativa sobre el servicio del Ayuntamiento, mediante cumplimentación de encuestas y presentación de sugerencias y reclamaciones

■ ■ Artículo 9. Deberes de la Ciudadanía

1. Deber de utilizar de buena fe los servicios y procedimientos de la Administración Electrónica.
2. Deber de facilitar al Ayuntamiento, en el ámbito de la Administración Electrónica, información veraz, completa y precisa, adecuada a los fines para los que se solicita.
3. Deber de identificarse por medios electrónicos adecuados en las relaciones administrativas con el Ayuntamiento, cuando éstas así lo requieran.
4. Deber de custodiar los elementos de identificación personal e intransferible utilizados en las relaciones administrativas por medios electrónicos con el Ayuntamiento.
5. Los ciudadanos que deseen que otra administración pública accedan a sus datos personales deberán suministrar su autorización expresa para el procedimiento específico.
6. Los ciudadanos que ejerzan el derecho a no aportar datos y documentos que obren en poder de la Administración Pública deberán expresar su consentimiento en los términos establecidos en el Artículo 6.2.b de la Ley 11/2007, para que la Sede Electrónica del Ayuntamiento pueda recabar los datos o documentos referidos al trámite específico que se encuentren en otra administración pública.
7. Los representantes de los ciudadanos deberán suministrar el documento que les autoriza, para actuar en todas sus relaciones con el Ayuntamiento.

■ ■ Artículo 10. Cumplimiento de derechos y deberes

El Ayuntamiento velará por el cumplimiento de los derechos y deberes de los ciudadanos, de acuerdo con lo establecido en las leyes: Ley 30/1992 y Ley 11/2007 y en las previsiones de esta Ordenanza.

■ **Capítulo 4º. La Sede Electrónica**

■ ■ Artículo 11. Características de la Sede Electrónica

1. Configuración

- a. La sede electrónica se configurará como el portal de servicios administrativos del Ayuntamiento de Leganés en su relación con la Ciudadanía.
- b. La Sede Electrónica contará con todo el equipamiento necesario para satisfacer los requerimientos establecidos en la Ley 11/2007.
- c. La Sede Electrónica del Ayuntamiento de Leganés se integrará en el Esquema Nacional de Interoperabilidad.
- d. La Sede Electrónica del Ayuntamiento de Leganés se integrará con el Esquema Nacional de Seguridad.

2. Plataforma tecnológica

- a. La Sede Electrónica cumplirá los estándares de accesibilidad, usabilidad y calidad recomendados para las Administraciones Públicas, y en particular se garantizará que los servicios, informaciones, trámites y procedimientos objeto de esta Ordenanza sean accesibles desde los principales navegadores y sistemas operativos existentes en el mercado.
- b. La plataforma tecnológica que soporte a la Sede Electrónica garantizará la confidencialidad, disponibilidad e integridad de los datos y documentos que en ella se ubiquen.

3. Acceso a la Sede Electrónica

Se accederá a través de la red Internet en el siguiente dominio Web: www.leganes.org y subdominios según determine el Ayuntamiento.

4. Operatividad

Los servicios de la Sede Electrónica estarán operativos las 24 horas del día, todos los días del año, exceptuando casos de fuerza mayor.

En los casos de interrupción de los servicios prestados por medio de la Sede Electrónica, se informará a los ciudadanos con la máxima antelación posible, por medio de la misma sede u otro medio, indicando cuáles son los medios alternativos de acceso disponibles, salvo excepciones puntuales imposibles de prever.

5. Calidad y seguridad

Los actos administrativos y resoluciones dictados por el Ayuntamiento y las comunicaciones con los ciudadanos que se realicen por medios electrónicos cumplirán los requisitos de seguridad, integridad y conservación previstos en el artículo 45.5 de la Ley 30/1992.

Se realizará la debida protección a los datos personales de los ciudadanos según lo establecido en la Ley 15/1999.

El Ayuntamiento de Leganés no será responsable en ningún caso de la información que se pueda obtener a través de fuentes externas que no dependan del mismo, ni tampoco de las opiniones que puedan expresar, a través de las páginas Web municipales, las personas no vinculadas a dichas entidades.

6. Interoperabilidad

A través de la sede electrónica del Ayuntamiento de Leganés, se podrá acceder a las Webs de otras administraciones públicas y obtener la información que estas ofrecen, facilitando así el acceso a la información y los distintos trámites a los ciudadanos.

■ ■ Artículo 12. Identificación de los interesados y autenticación de su actuación

1. La identificación de los interesados y autenticación de sus actos en su relación con el Ayuntamiento de Leganés a través de la Sede Electrónica, se realizará con algunos de los siguientes mecanismos:
 - a. DNI-e: Certificado electrónico incorporado al Documento Nacional de Identidad, de acuerdo con la normativa reguladora de dicho documento, para personas físicas.

- b. Los sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico emitido por la plataforma @firma de la Administración General del Estado.
 - c. Los certificados de firma electrónica emitidos por la Fábrica Nacional de Moneda y Timbre.
2. La utilización de cualquiera de los mecanismos de identificación y autenticación recogidos en este artículo será requisito suficiente para identificar y entender acreditada la voluntad de los ciudadanos que presenten escritos o documentos electrónicos en cualquier procedimiento o trámite en la Sede Electrónica.
 3. Las actuaciones autenticadas con las firmas electrónicas tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza.
 4. De conformidad con lo dispuesto en el artículo 71 de la Ley 30/1992, el Ayuntamiento requerirá de los ciudadanos la subsanación de cualquier defecto formal ocasionado por el incumplimiento de los requisitos de identidad, integridad y autenticidad previstos en este artículo.
 5. El uso de 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.
 6. El uso de sistemas de firma electrónica implicará el uso de los datos personales consignados incluidos en la firma electrónica, con el único fin de realizar la verificación de la firma.
 7. El Ayuntamiento podrá habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la presentación electrónica de documentos en representación de los interesados tal como lo establece el Artículo 23 de la Ley 11/2007.
 8. Las personas o entidades habilitadas para la representación de terceros deberán ostentar la representación necesaria para cada actuación, según lo establece el Artículo 32 de la Ley 30/1992 o en los términos que resulten de la normativa específica de la aplicación.

■ ■ Artículo 13. Identificación y autenticación de los órganos administrativos

De acuerdo con el artículo 13 de la Ley 11/ 2007 y del artículo 3 de la Ley 59/2003, la identificación y autenticación del ejercicio de competencia del personal al servicio del Ayuntamiento y de sus órganos administrativos de acuerdo a lo previsto en la Ley 30/1992 en su Artículo 45, la identificación y autenticación de los órganos de la administración y su personal, se realizará mediante la firma electrónica reconocida y será asignada en los siguientes niveles:

1. Firma certificada en forma conjunta de una unidad, servicio o grupo específico.
2. Firma individual al personal con competencia específica.
3. Todas las firmas electrónica asignada al personal contendrá información de la persona que la utilice, su ubicación administrativa, cargo y competencia.
4. El Ayuntamiento establecerá el control de asignación y supervisión de firmas electrónicas en el Ayuntamiento.

5. Se emitirán certificados de autenticación del organismo que corresponda en los procesos automatizados que no precisen la intervención del personal administrativo. Al certificado se le agregará un sellado de tiempo electrónico.

■ ■ **Artículo 14. Identificación y autenticación de las sedes electrónicas**

La Sede Electrónica del Ayuntamiento de Leganés, contendrá un sistema de firma electrónica basado en certificados de dispositivo seguro o medio equivalente.

El Ayuntamiento podrá realizar convenios con otras Administraciones Públicas con el fin de establecer las bases tecnológicas y administrativas para la identificación y autenticación de las sedes electrónicas de cada una de ellas.

■ **Capítulo 5º. *La difusión de la información administrativa por medios electrónicos***

■ ■ **Artículo 15. Acceso a la información**

El Ayuntamiento de Leganés garantizará a los ciudadanos el acceso a los servicios de difusión de la información en su ámbito de competencia, a través de diferentes canales, contando al menos con los siguientes medios:

1. La Sede Electrónica, a través de la cual los ciudadanos podrán acceder a todos los servicios de información disponibles por el Ayuntamiento.
2. Servicio 010, servicio de atención telefónica, que en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, facilitarán a los ciudadanos la misma información que se regula en la presente Ordenanza.
3. SAC móvil, en los horarios y ubicaciones establecidos para este servicio.
4. SAC presencial, en los horarios y ubicaciones establecidos para este servicio.

El acceso a la información en la Sede Electrónica será conforme a su clasificación basada en su tipo y uso, aplicando el principio de proporcionalidad con respecto a la protección de datos.

Los tipos de accesos para obtener información en la Sede Electrónica será la siguiente:

- a. Mediante firma electrónica, según lo regulado por esta ordenanza.
- b. Sin requerir identificación del solicitante.
- c. Con una suscripción previa, según el tipo de servicio.

■ ■ **Artículo 16. Información sobre la organización y servicios de interés general**

1. El Ayuntamiento de Leganés facilitará por medios electrónicos, como mínimo, a través de la Sede Electrónica, información sobre:
 - a. Su organización y sus competencias, considerando los órganos definidos en los artículos 35, 36, 37 del Reglamento Orgánico Municipal del Ayuntamiento de Leganés.

- b. Los servicios que tenga encomendados o asumidos, con la indicación de las prestaciones concretas y la disponibilidad de cada uno de los servicios.
 - c. Los procedimientos administrativos que tramitan con indicación de los requisitos esenciales y de los plazos de resolución y notificación, así como del sentido del silencio.
 - d. Los datos de localización, como son la dirección postal, el número de teléfono y horarios de atención por canal de prestación de servicios.
 - e. El texto actualizado de los Reglamentos y Ordenanzas.
 - f. Los medios electrónicos que los ciudadanos pueden utilizar en ejercicio de su derecho a comunicarse con este Ayuntamiento.
 - g. El tablón de anuncios electrónico.
 - h. El callejero actualizado.
2. Se podrá difundir a través de medios electrónicos cualquier otra información relativa a asuntos o cuestiones de interés general para los ciudadanos, incluida la que pueda contribuir a una mejor calidad de vida de los ciudadanos y tenga una especial incidencia social.
3. En la información facilitada se harán constar el órgano administrativo proveedor de la información, unidad administrativa responsable y las fechas de actualización.

El Ayuntamiento de Leganés garantizará la disponibilidad y el acceso a su ordenanza a través de Internet.

■ ■ **Artículo 17. Información administrativa**

1. El Ayuntamiento facilitará a través de medios electrónicos toda la información administrativa que por prescripción legal o resolución judicial se tenga que hacer pública por este medio, y se especificará en todos los casos el órgano administrativo autor del acto o disposición publicados.
2. El acceso a los documentos y expedientes almacenados en la Sede Electrónica que contengan datos referentes a intimidad de las personas estará reservada a estas.
3. Los ciudadanos en su carácter de participantes en trámites o solicitudes, podrán obtener información sobre documentos, expedientes y estado de los procedimientos siempre que se identifiquen por los medios estipulados.
4. Los ciudadanos podrán consultar los documentos electrónicos almacenados en la Sede Electrónica que hagan referencia a procedimientos finalizados en la fecha de consulta y no contengan información referida a la intimidad de las personas.
5. El derecho de acceso a la información será ejercido por los particulares de forma que no se vea afectada la eficacia del funcionamiento de los servicios del Ayuntamiento, en tal caso se deberá formular petición individualizada de los documentos o expedientes que se deseen consultar.
6. La información administrativa que estará accesible en la Sede Electrónica se presenta en el anexo II. Por resolución de Alcaldía se especificará la información administrativa que estará accesible en la Sede Electrónica

■ ■ Artículo 18. Tablón de edictos electrónico

La publicación de disposiciones administrativas, boletines oficiales y anuncios, que por disposición legal o reglamentaria se deba publicar en el tablón de edictos, se irá implementando en la Sede Electrónica en la medida de las posibilidades técnicas y presupuestarias del Ayuntamiento.

Una vez implementada la totalidad del tablón de edictos en la Sede Electrónica, la publicación en papel podrá ser eliminada, según se establece en la ley 11/2007 en su Artículo 12.

La información y contenidos del tablón de edictos electrónico, será de libre acceso para todos los ciudadanos.

El Ayuntamiento garantizará la autenticidad e integridad del contenido del tablón de edictos electrónico y el mismo tendrá carácter oficial y autentico tal como lo establece la Ley 30/1992 en su Artículo 45.5.

El Ayuntamiento de Leganés podrá convenir con las otras Administraciones Públicas para establecer los procesos electrónicos para el intercambio de los edictos del tablón, como medida de cooperación para la ejecución de sus respectivas competencias, según se establece en la Ley 30/1992, en su Artículo 4.

■ ■ Artículo 19. Publicación oficial

En la medida de las posibilidades presupuestarias, el Ayuntamiento irá implantando módulos de información general referente a los siguientes aspectos:

1. Información completa sobre las campañas del Ayuntamiento.
2. Información general sobre los servicios que presta el Ayuntamiento.
3. Otras informaciones que el Ayuntamiento considere conveniente para el bienestar de los ciudadanos.

■ **Capítulo 6º. Oficina virtual, registro, comunicaciones y notificaciones electrónicas**

■ ■ Artículo 20. Oficina Virtual

1. La Oficina Virtual es el canal de acceso a los servicios electrónicos del Ayuntamiento de Leganés para los que se precisa identificación previa. El acceso se efectuará autenticando la personalidad por medio del DNI electrónico o el certificado digital correspondiente. La Oficina Virtual será parte integrante de la Sede Electrónica.

Los ciudadanos podrán utilizar los procesos electrónicos que ofrece la Oficina Virtual como medio de comunicación e interlocución con el Ayuntamiento para servicios tales como:

- a. Acceder a la información personalizada del ciudadano que se identifica.
- b. Realizar operaciones y/o trámites administrativos de servicios o procedimientos gestionados por el Ayuntamiento de Leganés y que se tramiten de forma electrónica.
- c. Aportar y gestionar los datos facilitados para sus relaciones con el Ayuntamiento de Leganés: teléfonos, correos electrónicos y direcciones así como el canal que prefiere para recibir información del Ayuntamiento de Leganés.

Estos datos contarán con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999 y su normativa de desarrollo.

2. El acceso y utilización de la Oficina Virtual presupone que la persona usuaria ha leído el contenido de las normas y condiciones de uso de la Sede Electrónica, en el momento de acceso, y que las acepta de forma expresa, plena y sin reservas. Dichas normas y condiciones deberán ser aceptadas la primera vez que se accede o en aquellos casos en que éstas sean modificadas con posterioridad a su aceptación. El Ayuntamiento será responsable de comunicar la existencia de una nueva versión de las normas y condiciones de uso. En caso de no estar de acuerdo con el contenido de las nuevas normas el usuario tendrá que abandonar este canal de prestación de servicios personales y comunicarlo al Ayuntamiento.
3. El Alcalde Presidente, aprobará mediante resolución, y previa tramitación del expediente administrativo, las normas de utilización de la Oficina Virtual así como los canales a través de los que se podrá acceder a esta Oficina Virtual. Se podrá acceder a la Oficina Virtual a través de la Sede Electrónica y del canal telefónico. Progresivamente se incorporarán nuevos canales en función del desarrollo tecnológico y de la configuración de los servicios.

■ ■ Artículo 21. Registro Electrónico de entrada y salida de documentos

1. De conformidad con el artículo 24.1 y 25 de la Ley 11/2007 y el Art. 49 de la Ley 7/85 de 2 de abril Reguladora de las Bases de Régimen Local, mediante esta Ordenanza se crea y regula el funcionamiento del Registro Electrónico del Ayuntamiento de Leganés, de acuerdo con las siguientes normas:
 - a. El Registro Electrónico tendrá carácter voluntario para los ciudadanos, a excepción de los supuestos de utilización obligatoria establecidos por Ley y/o normas de creación de futuros procedimientos electrónicos donde se regule la presentación de solicitudes, escritos o comunicaciones a través del Registro Electrónico. Se accederá a través de la Sede Electrónica del Ayuntamiento de Leganés mediante la conexión a la dirección de Internet <http://www.leganes.org>. Las disposiciones que aprueben la incorporación de trámites y procedimientos por vía electrónica determinarán qué documentos y formatos tendrán entrada en el Registro Electrónico, así como sus condiciones de funcionamiento.
 - b. En el Registro Electrónico se podrán presentar solicitudes, escritos o comunicaciones relativos a los procedimientos administrativos y asuntos que sean competencia del Ayuntamiento. Por resolución de Alcaldía se especificarán los trámites y asuntos disponibles en Sede Electrónica.

A tal efecto, se adoptarán las medidas oportunas para que las oficinas de registro físicas, a que se refiere el artículo 38 de la Ley 30/ 1992, del Ayuntamiento de Leganés garanticen la interconexión de todas sus oficinas y se posibilite el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

- c. En el Registro Electrónico, la fecha de entrada y/o de salida, el número y la hora, se acreditará mediante un servicio de consignación electrónica. Se procederá a la anotación de los correspondientes asientos de entrada y salida de acuerdo con lo dispuesto en el 38 de la Ley 30/ 1992 y en el artículo 153 y siguientes del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.
- d. Se procederá al mantenimiento y conservación de un archivo informático de los asientos de entrada y salida de solicitudes, escritos y comunicaciones electrónicas, correspondiente al año natural.

- e. En la dirección electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones que pueden presentarse y se dará la oportuna publicidad para su conocimiento general. El número y tipo de solicitudes que se puedan presentar a través del Registro Electrónico no será inferior al que se puedan presentar por el canal presencial y por el canal telefónico, incorporándose progresivamente los canales que se aprueben. La presentación de solicitudes, escritos y comunicaciones en el Registro Electrónico, tendrá idénticos efectos que la efectuada por los demás medios admitidos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, LRJ-PAC.
- f. Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación siempre que cumplan los estándares de formato y requisitos de seguridad.
- g. Cualquier solicitud, escrito o comunicación que los interesados presenten a través del Registro Electrónico y que no esté relacionado con los procedimientos y asuntos mencionados no producirá ningún efecto y se tendrá por no presentado, comunicándose al interesado esta circunstancia e indicándole los registros y, en su caso, los lugares habilitados para su presentación de acuerdo con el artículo 38.4 de la Ley 30/1992.
- h. En ningún caso tendrán la condición de Registro Electrónico los buzones de correo electrónico corporativos asignados a los empleados públicos o a las distintas unidades y órganos. Tampoco tendrán consideración de Registro Electrónico los dispositivos de recepción de fax.

■ ■ Artículo 22. Escritos y documentos susceptibles de registro de entrada

1. Son susceptibles de registro de entrada las solicitudes, escritos y comunicaciones en las que quede correctamente identificado tanto el remitente como la persona, órgano, medio de presentación, procedimiento o unidad administrativa del Ayuntamiento a la que se dirige.
2. Cuando la interesada o interesado deba adjuntar determinada documentación para la debida tramitación de su solicitud o escrito, ésta podrá aportarse en soporte electrónico si van firmados electrónicamente por la propia persona interesada o por terceros que vengán autenticados a través de la firma electrónica reconocida.

En caso contrario, dicha documentación deberá de presentarse en el plazo máximo de diez días hábiles en soporte papel original o copia compulsada del documento, en cualquiera de las oficinas de registro del Ayuntamiento y en los demás lugares que establece el artículo 38.4 de la Ley 30/1992, indicando el número de registro de entrada asignado por la unidad registral electrónica de la solicitud o escrito a la que se adjunta dicha documentación.

3. Todos los documentos deberán ser compatibles en formato con los utilizados por el Ayuntamiento y estar realizado por aplicaciones informáticas compatibles. El tipo de formatos y aplicaciones informáticas admisibles se aprobarán por resolución de Alcaldía y se publicarán en la Sede Electrónica del Ayuntamiento. Siendo el formato estándar admitido pdf y un tamaño máximo en total por registro o entrega de 4 MB.
4. La no aportación de documentos en el plazo anteriormente señalado, desestimaré la solicitud formulada y se remitirá en soporte electrónico a la interesada o interesado la resolución que así lo declare, si éste hubiera sido el medio señalado por el mismo como preferente o consentido, o por cualquier medio que permita tener constancia de la recepción del interesado o la interesada o la persona representada, con los efectos previstos en el artículo 42 de la Ley 30/1992.
5. Se podrán rechazar los documentos electrónicos que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.

6. En los casos previstos en los apartados anteriores, 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 a la que pueda presentarse. Cuando el interesado lo solicite se remitirá justificación del intento de presentación, que incluirá las circunstancias de su rechazo.

■ ■ Artículo 23. Cómputo de plazos en Registro Electrónico

1. El Registro Electrónico del Ayuntamiento de Leganés se regirá, a efectos de cómputo de plazos, por la fecha y la hora oficial de la Sede Electrónica, que contará con las medidas de seguridad necesarias para garantizar su integridad y figurar visible en la dirección electrónica de acceso al Registro.
2. Estará a disposición de los usuarios y usuarias las veinticuatro horas del día, todos los días del año, excepto las interrupciones que sean necesarias por razones técnicas.
3. A los efectos de cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, habrá que considerar lo siguiente:
 - a. La fecha y hora de referencia serán los vigentes en el momento de la recepción o salida de la correspondiente solicitud, escrito o comunicación, en el sistema de información que dé soporte al Registro Electrónico.
 - b. La entrada de solicitudes, escritos y/o comunicaciones recibidas en días inhábiles se entenderán efectuadas en la primera hora del primer día hábil siguiente. Constará en el asiento de entrada correspondiente la fecha y hora en que efectivamente se ha recibido la solicitud, escrito o comunicación presentada pero se indicará en el mensaje de confirmación las cero horas y un minuto del siguiente día hábil.
 - c. El inicio del cómputo de los plazos que hayan de cumplir los órganos del Ayuntamiento vendrá determinado por la fecha y hora de presentación en el propio registro.
 - d. Se consideran días inhábiles, a efectos del Registro Electrónico del Ayuntamiento, los establecidos como días festivos en el calendario oficial de fiestas laborales de la Comunidad Autónoma de Madrid y fiestas locales de este Municipio. Este calendario estará publicado en la sede electrónica. En todo caso no será de aplicación al Registro Electrónico lo dispuesto en el artículo 48.5 de la Ley 30/1992.
 - e. Los programas, aplicaciones y sistemas de información que en cada caso se utilicen para la realización por medios electrónicos de los trámites administrativos garantizarán el control de los plazos, la constancia de la fecha y hora y la identificación de las personas responsables de las actuaciones, además de respetar el orden de tramitación de los expedientes.

■ ■ Artículo 24. Régimen de funcionamiento del Registro Electrónico

1. Cualquier anomalía de tipo técnico que se detecte en la recepción electrónica del documento, deberá darse a conocer al usuario por parte del propio sistema, mediante el correspondiente mensaje de error, a fin de que le conste que no se ha producido válidamente la presentación.
2. Se emitirá automáticamente un justificante de la recepción de los documentos electrónicos presentados por los ciudadanos, que consistirá en una copia auténtica del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro. A dicho justificante se podrá acceder, consultar e imprimir desde la Oficina Virtual, autenticando los datos de registro que se le asignen.

3. La recepción de solicitudes, escritos y comunicaciones se podrá interrumpir por el tiempo imprescindible, sólo cuando concurren razones justificadas de mantenimiento técnico u operativo. Cuando por razones técnicas se prevea que el registro no puede estar operativo, se deberá informar a los usuarios del Registro Electrónico con la máxima antelación posible y mientras dure esta situación, publicándose en la Sede Electrónica. En los supuestos de interrupción no planificada en el funcionamiento del Registro Electrónico y siempre que sea posible, la persona usuaria visualizará un mensaje en que se comunique tal circunstancia.
4. El Ayuntamiento podrá eliminar aquellos documentos o solicitudes que supongan un riesgo para la seguridad del sistema. En ese caso, no se tendrá por presentado el documento o solicitud.

■ ■ **Artículo 25. Autenticidad, integridad, confidencialidad, disponibilidad y conservación del contenido de los asientos electrónicos**

- a. El sistema informático soporte del Registro Electrónico del Ayuntamiento garantizará la autenticidad, integridad, confidencialidad, disponibilidad y conservación de los asientos practicados.
- b. En la remisión de escritos, solicitudes y comunicaciones que se realicen a través del Registro Electrónico a los órganos competentes o desde éstos hacia los interesados, se adoptarán las medidas de seguridad necesarias para evitar la interceptación y alteración de las comunicaciones, los accesos no autorizados y garantizar la protección de los datos de carácter personal, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999 y el Real Decreto 1720/2007, de 21 de diciembre que la desarrolla.
- c. Asimismo, el sistema informático de soporte del Registro Electrónico del Ayuntamiento informará a todos aquellos órganos de la administración y a los ciudadanos que deseen acceder al mismo, que la presentación de escritos, solicitudes y comunicaciones de forma electrónica supone la comunicación de sus datos personales a los órganos administrativos o entidades competentes para su recepción y tramitación.

■ ■ **Artículo 26. Las comunicaciones electrónicas**

1. Las comunicaciones electrónicas se practicarán a través de la Oficina Virtual de la Sede Electrónica y deberán de cumplir los siguientes requisitos:
 - a. Las comunicaciones a través de la Oficina Virtual en los procedimientos administrativos y trámites electrónicos, requerirán solicitud expresa por parte del interesado para la utilización de estos medios, excepto en los casos en los que una norma con rango de Ley establezca o infiera la utilización de un medio no electrónico. Los ciudadanos podrán, en cualquier momento optar por un medio distinto del inicialmente elegido.
 - b. Será necesario que el interesado disponga de una dirección de correo electrónico válida y única de manera que se garantice exclusividad de su uso y la identidad del usuario. Esta dirección tendrá vigencia indefinida como dirección válida a efectos de notificación, excepto en los supuestos en que el titular solicite su revocación o modificación, por defunción de la persona física o extinción de la personalidad jurídica, cuando una resolución administrativa o judicial así lo ordene.
 - c. Las comunicaciones se podrán consultar, una vez identificado y aceptadas las normas de utilización, desde la Oficina Virtual del Ayuntamiento de Leganés
2. Las diferentes concejalías o áreas que componen el Ayuntamiento deberán utilizar preferentemente medios electrónicos para comunicarse entre ellos, así como para su comunicación con otras Administraciones Públicas atendiendo a los siguientes puntos:

- a. 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 personas emisoras y receptoras en las condiciones establecidas en el presente artículo.
 - b. Cuando las personas participantes en las comunicaciones pertenezcan al Ayuntamiento, se determinarán las condiciones y garantías en que se registrarán y comprenderán al menos la relación de personas emisoras y receptoras autorizadas y la naturaleza de los datos a intercambiar. Si quienes participen pertenecen a distintas administraciones estas condiciones se establecerán mediante convenio.
 - c. En todo caso se garantizará la seguridad del entorno cerrado de comunicaciones la protección de los datos que se transmitan.
3. 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.

■ ■ Artículo 27. Las notificaciones electrónicas

1. La notificación se podrá practicar utilizando medio electrónico, cuando el interesado haya señalado dicho medio como preferente o haya consentido su utilización en los procedimientos administrativos y trámites incorporados a la tramitación por vía electrónica. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citado anteriormente podrá emitirse y recabarse, en todo caso, por medios electrónicos.
2. 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 Ayuntamiento.
3. Para la validez de las notificaciones será necesario que el interesado manifieste su voluntad de recibir notificación por medios electrónicos y disponga de una dirección de correo electrónico habilitada para aquella finalidad, que será única para cada interesado y cumpla los requisitos legalmente previstos en el artículo 59 de la Ley 30/1992.
4. La notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el acceso a su contenido en la dirección de correo electrónico. El sistema de notificación deberá acreditar las fechas y horas en que se produzca la recepción de la notificación en la dirección electrónica del interesado y el acceso al contenido del mensaje de notificación por parte del ciudadano, así como cualquier causa técnica que imposibilite alguna de las circunstancias anteriores.
5. Cuando haya constancia de la recepción de la notificación en la dirección electrónica y transcurran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada a los efectos previstos en el artículo 59.4 de la Ley 30/1992, y normas concordantes salvo que de oficio o a instancia del interesado se compruebe la imposibilidad técnica o material del acceso a su dirección electrónica.
6. Durante la tramitación de los procedimientos, el interesado podrá requerir al órgano o entidad correspondientes que las notificaciones sucesivas no se practiquen por medios electrónicos, en cuyo caso se deberá usar cualquier otro medio admitido por el artículo 59 de la Ley 30/1992. Igualmente, durante la tramitación de un procedimiento no electrónico, el interesado podrá requerir al órgano o entidad correspondientes que las notificaciones sucesivas se practiquen en la forma prevista en la presente Ordenanza.

7. El acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, producirá los efectos propios de la notificación por comparecencia electrónica en la Sede, siempre que quede constancia del acceso. El acceso al contenido de las actuaciones administrativas se realizará desde el apartado correspondiente de la Oficina Virtual previa identificación y aceptación de las normas de utilización.
8. 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 recursos que procedan, a partir de la primera de las notificaciones correctamente practicada. Se podrá advertir de este modo en el contenido de la propia notificación.

■ **Capítulo 7º. Los documentos y archivos electrónicos**

■ ■ **Artículo 28. Documento Administrativo electrónico**

1. El Ayuntamiento de Leganés establecerá los mecanismos necesarios para la emisión por medios electrónicos de documentos administrativos a los que se refiere el Art. 46 de la Ley 30/1992, que producirán idénticos efectos que los expedidos en soporte papel, siempre que incorporen una o varias firmas electrónicas tal y como se establece en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. El contenido de éstos se podrá imprimir en soporte papel y la firma manuscrita será sustituida por un código de verificación generado electrónicamente, que permitirá comprobar su autenticidad accediendo electrónicamente a los archivos del órgano u organismo emisor.
2. Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos, cuando la naturaleza del documento así lo requiera y podrán contener información de cualquier naturaleza. Asimismo deberán disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.
3. El Ayuntamiento emitirá documentos electrónicos sobre los datos que figuran en su poder a petición de los ciudadanos, mediante la actuación administrativa automatizada o mediante la actuación del personal municipal.
4. Los documentos electrónicos susceptibles de ser integrados en un expediente electrónico, deberán tener asociados metadatos que permitan su contextualización en el marco del Ayuntamiento, la función y el procedimiento administrativo al que corresponde, entendiendo como metadato cualquier tipo de información electrónica asociada a los documentos 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.
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.

■ ■ Artículo 29. Copias Electrónicas.

1. Se considerarán copias auténticas con la eficacia prevista en el Art. 46 de la Ley 30/1992 a las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el interesado o por el Ayuntamiento, 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. Los documentos electrónicos generados por el Ayuntamiento contarán con un código electrónico de verificación que permitirá la consulta de los mismos para comprobar la coincidencia del documento electrónico con el almacenado en el Archivo Electrónico.
2. El Ayuntamiento podrá 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 conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá realizarse de forma automatizada, mediante el correspondiente sello electrónico.
3. Se podrán emitir copias electrónicas con la consideración de copias auténticas de documentos electrónicos emitidos por el propio interesado o por el Ayuntamiento, así como copias auténticas electrónicas de documentos soporte papel, asegurando siempre la exactitud del contenido, autenticidad e integridad del documento original mediante firma electrónica reconocida y siempre y cuando se incluya un manifiesto relativo a la comprobación de los elementos de autenticidad e integridad del documento original.

■ ■ Artículo 30. Compulsas electrónicas de documentos en soporte papel

La compulsas electrónicas es el procedimiento de digitalización de los documentos en soporte papel, bien a través de procesos manuales o bien automatizados, que produce una copia electrónica auténtica del documento.

1. La compulsas electrónicas se realizará a través de un procedimiento de digitalización seguro, que incluya la firma electrónica reconocida del personal del Ayuntamiento que haya realizado la compulsas y que garantice la autenticidad y la integridad de la copia, así como la identificación del órgano que la realiza, mediante la firma electrónica correspondiente.
2. Se comunicará a los ciudadanos la puesta a disposición de los originales para su retirada del Ayuntamiento de Leganés. Transcurrido el plazo para la retirada de los documentos originales en soporte papel, que se comunicará al interesado en el momento de su presentación y una vez convertidos a formato electrónico y compulsados electrónicamente, se procederá a la destrucción de los mismos de acuerdo con los criterios establecidos por el Ayuntamiento. Se faculta al Alcalde Presidente a aprobar las series y tipos documentales que, por su valor histórico, no podrán ser destruidos y que serán enviados al Archivo Electrónico del Ayuntamiento de Leganés para su gestión.
3. Los documentos compulsados electrónicamente podrán ser válidos tanto en el procedimiento concreto para el que se ha realizado la compulsas como para cualquier otro procedimiento tramitado por el Ayuntamiento.

■ ■ Artículo 31. Archivo Electrónico

El Archivo Electrónico tiene como misión la conservación, organización y servicio de los documentos producidos y recibidos por el Ayuntamiento en el ejercicio de sus funciones, según indica el artículo 24.1 de la Ley 4/1993, de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid.

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas garantizando la identidad e integridad de la información que contienen y asegurando, en todo caso, la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones, de manera que se cumplan los términos previstos en el artículo 45.5 de la Ley 30/1992. La reproducción en soporte electrónico de documentos en soporte papel se hará de conformidad con el procedimiento de compulsas previsto en esta Ordenanza.
2. Los documentos en soporte informático, resultantes de la aportación al Ayuntamiento de información, solicitudes, certificados electrónicos y documentos por parte del interesado, o que hayan sido obtenidos mediante comunicaciones de datos administrativos de terceras administraciones, deben ser gestionados y archivados exclusivamente en soporte informático, de acuerdo con las prescripciones de la normativa legal de aplicación a este tipo de documentos.
3. Los medios, equipos y soportes en que se almacenen los documentos electrónicos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad y la conservación de los documentos archivados.
4. Los documentos originales en soporte informático podrán transformarse, adaptando el formato a las necesidades de gestión y preservación previstas al servicio, de acuerdo con las siguientes normas:
 - a. El cambio de formato deberá garantizar la exactitud del contenido del documento, así como la comprobación de los elementos de autenticidad e integridad del documento original. El documento resultante de la transformación será firmado electrónicamente por el órgano competente para la transformación.
 - b. El paso del documento en soporte informático a papel sólo se realizará excepcionalmente, y deberá permitir la verificación técnica de la firma del órgano competente para la transformación.
5. El Ayuntamiento determinará las normas de creación, organización y gestión del Archivo Electrónico, los criterios de migración de los datos, la renovación de los soportes, las actualizaciones de los programas así como las estrategias para garantizar la lectura de los documentos con el transcurso del tiempo
6. La preservación y el acceso a los documentos almacenados en medios electrónicos se regirá por las previsiones de esta Ordenanza relativas al acceso a la información y por los principios y normas aplicables a la protección de la confidencialidad y privacidad de datos, así como por los dictámenes del órgano municipal encargado de la evaluación y el acceso a los documentos.
7. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los y las particulares se conservarán en soportes electrónicos, ya sea en el mismo formato 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.
8. El archivo de documentos electrónicos se realizará de acuerdo con la normativa vigente en materia de gestión documental en lo relativo al cuadro de clasificación, método de descripción y calendario de conservación.
9. El Archivo Electrónico del Ayuntamiento tendrá como funciones principales: la descripción documental (metadatos), la gestión de fondos (transferencias, migraciones, selección y evolución), la gestión de usuarios, las auditorías de uso y circulación de documentos, la gestión de accesos (protección y seguridad de datos) y el control de autenticidad e integridad documental (validez jurídica).

10. El Ayuntamiento no se responsabilizará del uso fraudulento que los usuarios puedan llevar a cabo de los servicios prestados mediante administración electrónica. Los usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su autenticación en el acceso a estos servicios de 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. Será responsabilidad del usuario la adecuada custodia y manejo de los ficheros que le sean devueltos por el Registro Electrónico como recibo de presentación.
11. Los períodos mínimos de conservación de los documentos electrónicos se determinarán por el Ayuntamiento 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 del Ayuntamiento de Leganés.

■ ■ Artículo 32. Expediente electrónico

1. Es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.
2. Los expedientes electrónicos dispondrán de un código que permita su identificación unívoca por cualquier órgano de la Administración en un entorno de intercambio interadministrativo.
3. El foliado de los expedientes electrónicos podrá llevarse a cabo mediante un código electrónico, firmado o sellado por el órgano actuante. Este código garantizará la integridad del expediente electrónico y permitirá su fácil recuperación, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.
4. 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 en soporte papel.
5. Los expedientes electrónicos estarán integrados por documentos electrónicos, que se ajustarán al formato o formato de larga duración y que podrán formar parte de distintos expedientes, pudiendo incluir asimismo otros expedientes electrónicos si así lo requiere el procedimiento.

■ Capítulo 8º. *Gestión electrónica de los procedimientos. Disposiciones comunes*

■ ■ Artículo 33. Trámites y procedimientos a los que es aplicable la tramitación electrónica

1. Una vez que se apruebe y entre en vigor esta Ordenanza, podrán tramitarse electrónicamente:
 - a. Los procedimientos administrativos que se aprueben por resolución de Decreto de Alcaldía.
 - b. La consulta de datos en poder del Ayuntamiento por parte de los ciudadanos.
 - c. Las comunicaciones de los ciudadanos, en especial avisos, quejas, sugerencias y peticiones, no englobadas en un procedimiento administrativo.
 - d. La presentación de solicitudes y aportación de documentos a través del Registro Electrónico.

2. La relación actualizada de procedimientos, trámites, solicitudes, escritos y comunicaciones que se podrán tramitar electrónicamente será accesible a través de la Sede Electrónica, junto con los criterios de cumplimiento de trámites de los diferentes procedimientos, consulta del estado de tramitación, así como la comunicación de avisos de interés dentro de los procedimientos.
3. La tramitación de un procedimiento administrativo por medios electrónicos no podrá suponer ninguna merma en el mantenimiento de la integridad de las garantías jurídicas de los particulares ante las Administraciones Públicas establecidas en el Ordenamiento Jurídico y, en particular, en la Ley 30/1992.
4. El Ayuntamiento de Leganés incorporará progresivamente los trámites y procedimientos administrativos municipales a la tramitación por vía electrónica, conforme al procedimiento de incorporación y a los principios generales de actuación previstos en esta Ordenanza.

■ ■ **Artículo 34. Mecanismo de incorporación de trámites y procedimientos a la tramitación por vía electrónica**

1. El Ayuntamiento de Leganés acordará la utilización de medios electrónicos en la actividad administrativa respetando la titularidad y el ejercicio de competencia del órgano responsable y cumpliendo siempre los requisitos establecidos en las normas que regulen la correspondiente actividad, fomentando los criterios de simplificación administrativa para impulsar la aplicación de medios electrónicos a los procesos de trabajo, en la gestión de los procedimientos y de la actuación administrativa.

La aplicación de medios electrónicos a la gestión de procedimientos, procesos y servicios irá precedida siempre de un análisis de rediseño funcional y simplificación del procedimiento, procesos o servicios.

2. Por resolución de Decreto de Alcaldía, se podrá aprobar la progresiva incorporación de procedimientos electrónicos con el objeto de garantizar una tramitación plena de procedimientos administrativos.
3. El proyecto de incorporación deberá contener:
 - a. Identificación de los trámites y procedimientos que se incorporan.
 - b. Identificación de los canales electrónicos habilitados para la realización del trámite.

■ **Capítulo 9º. Utilización de medios electrónicos en la tramitación del procedimiento**

■ ■ **Artículo 35. Iniciación del procedimiento administrativo**

1. Los procedimientos administrativos incorporados a la tramitación por vía electrónica se podrán iniciar mediante la presentación de solicitud, normalizada o no, en el Registro Electrónico regulado en esta Ordenanza. Dichas solicitudes electrónicas deberán contener la firma electrónica reconocida de la persona interesada o cualquier otro mecanismo de identificación y de acreditación de la voluntad del ciudadano, de conformidad con lo previsto en el artículo 70 de la Ley 30/1992,.
2. Los interesados podrán aportar al expediente copias digitalizadas de los documentos que sean necesarios o estimen oportunos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada o con una declaración del interesado. El Ayuntamiento podrá en cualquier momento requerir al interesado la exhibición

del documento o de la información original, pudiendo solicitar el cotejo del contenido de las copias aportadas con el archivo correspondiente. 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, y/o pertenecientes a otras Administraciones, pudiendo ofrecer un formulario cumplimentado con la información disponible, con objeto de que el interesado verifique la información y, en su caso, la modifique y complete.
4. El Ayuntamiento pondrá a disposición de las personas interesadas, en la iniciación de un procedimiento administrativo por medios electrónicos, los correspondientes modelos o sistemas electrónicos de solicitud en la Sede Electrónica que serán accesibles, sin otras restricciones tecnológicas que las derivadas de la utilización de estándares y criterios de comunicación y seguridad de acuerdo con las normas y protocolos nacionales.

■ ■ Artículo 36. Representación

1. Cuando en una solicitud electrónica haya más de un interesado, la solicitud deberá acompañar un documento electrónico con la autorización expresa de la representación. Las actuaciones se seguirán con el que se haya señalado expresamente o, en su defecto, con el interesado que aparezca encabezando la solicitud.
2. Los ciudadanos podrán actuar por medio de representantes en los procedimientos y trámites administrativos que se realicen frente al Ayuntamiento por medios electrónicos, de acuerdo con lo previsto por la legislación general y lo que establece esta Ordenanza. En estos supuestos, la validez de las actuaciones realizadas estará sujeta a la acreditación de la representación, que podrá realizarse mediante la aportación de documento electrónico pudiendo ser validado con posterioridad a su presentación por el Ayuntamiento.
3. Cualquier persona física con capacidad de obrar puede representar por vía electrónica a otras personas, físicas o jurídicas, siempre que acredite la citada representación mediante uno de los mecanismos alternativos válidos para ello.
4. El Ayuntamiento de Leganés, podrá habilitar con carácter general o específico a personas físicas o jurídicas para la realización de determinadas transacciones electrónicas en representación de las personas interesadas. Dicha habilitación deberá especificar las condiciones y obligaciones a 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.

El Ayuntamiento podrá requerir, en cualquier momento, la acreditación de dicha representación.

■ ■ Artículo 37. Tramitación del procedimiento administrativo

1. Los programas, aplicaciones y sistemas de información que se utilicen para la realización de trámites administrativos por medios electrónicos deberán garantizar el control de plazos, la constancia de la fecha y hora, 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. Cualquier actuación del interesado y los actos administrativos hechos en un procedimiento administrativo electrónico deberán de reunir los requisitos de validez legalmente establecidos con carácter general, así como ser emitidos o recibidos a través del Registro Electrónico que se regula en la presente Ordenanza.
3. Los órganos administrativos deberán garantizar el derecho de los interesados a formular alegaciones a través de medios electrónicos, así como el derecho de audiencia y de información pública a los ciudadanos.
4. De acuerdo con los principios de simplicidad administrativa e interoperabilidad entre Administraciones, las entidades comprendidas en el ámbito de aplicación de esta Ordenanza promoverán la eliminación de certificados y documentos en papel, que serán sustituidos, siempre que sea posible, por certificados y documentos electrónicos o por transmisiones de datos, con plena validez y eficacia siempre que se acredite la identidad, integridad, autenticidad y confidencialidad de los datos mediante los correspondientes certificados de firma electrónica reconocida. No siendo necesario aportar documentos que se encuentren en poder del Ayuntamiento o de otras Administraciones Públicas con las que se haya firmado un convenio de colaboración. El ejercicio de este derecho se hará de acuerdo con la normativa aplicable a cada procedimiento.
5. Tanto en el caso de certificados y documentos electrónicos como en el de transmisiones de datos, su expedición, tratamiento y efectos, se regirán por lo dispuesto en esta Ordenanza, con estricta sujeción a la normativa de protección de datos de carácter personal, así como al resto de la normativa aplicable al procedimiento administrativo.

El Ayuntamiento promoverá el establecimiento de convenios con las entidades públicas o privadas, tanto emisoras como receptoras de certificados o documentos administrativos, para simplificar la obtención, la transmisión y la convalidación de documentos o certificados electrónicos por transmisiones de datos. La aportación de certificados que prevén las normas reguladoras vigentes de procedimientos y actuaciones administrativas se podrá realizar a través de certificados electrónicos, con plena validez y eficacia, de acuerdo con las siguientes precisiones:

- a. En el marco de un procedimiento administrativo, el Ayuntamiento de Leganés, como responsable del trámite, podrá solicitar electrónicamente la transmisión de datos en poder de otras administraciones que sean necesarias para el ejercicio de sus competencias.
- b. Para dar respuesta a las peticiones de las administraciones con convenios, el Ayuntamiento dispondrá de mecanismos automáticos de transmisión de datos en tiempo real.
- c. Cualquier transmisión de datos, hecha por el Ayuntamiento de Leganés u otras administraciones, se efectuará a solicitud del órgano o entidad tramitadora. Se identificarán los datos requeridos y a sus titulares, así como la finalidad para la que se requieren. En la solicitud debe constar que se dispone del consentimiento expreso de las personas titulares afectadas, de la manera prevista en el apartado anterior, salvo que este consentimiento no sea necesario, en virtud de una norma con rango de ley.
- d. Quedará constancia de la petición y recepción de los datos en el expediente, por parte del órgano u organismo receptor. Para la verificación del origen y la autenticidad de los datos por parte de los órganos de fiscalización y control, se habilitarán mecanismos para que dichos órganos puedan realizar los controles oportunos.
- e. Tanto la petición como la transmisión de datos deberán ir acompañadas de la firma electrónica reconocida del órgano administrativo competente para garantizar la identidad de la administración peticionaria y la de la administración emisora, así como asegurar la integridad, autenticidad y confidencialidad de los datos transmitidos.

6. Para la sustitución de un certificado en papel por la transmisión de los datos correspondientes, el titular de éstos tiene que haber consentido expresamente la realización de la transmisión, de acuerdo con lo que establece la normativa de protección de datos de carácter personal, excepto en los casos previstos en una norma con rango de ley. Si no presta su consentimiento, el interesado deberá solicitar y aportar el certificado correspondiente.
7. La aportación en papel u otro soporte físico de documentos en un procedimiento administrativo electrónico, deberá dejar constancia del número o código de registro individualizado correspondiente a aquel procedimiento en el Registro Electrónico.
8. Las entidades comprendidas en el ámbito de aplicación de esta Ordenanza promoverán la sustitución de la aportación de documentos acreditativos del cumplimiento de requisitos por una declaración responsable del interesado, que exprese la concurrencia de dichos requisitos y el compromiso de aportar los justificantes, a requerimiento de la Administración.

■ ■ **Artículo 38. Continuación del procedimiento administrativo electrónico por medios tradicionales**

1. Cuando un procedimiento iniciado electrónicamente no se pueda tramitar totalmente en soporte electrónico se procederá, por parte del órgano competente a la reproducción en soporte papel de las solicitudes, comunicaciones u otros documentos electrónicos, para poder continuar con la tramitación del expediente, asegurándose en cualquier caso el archivo seguro de los documentos electrónicos originales.
2. Para garantizar la concordancia entre los documentos electrónicos originales y los reproducidos en papel, en toda copia se dejará constancia de la diligencia del funcionario competente que acredite la correspondencia y exactitud con el documento original. Estos documentos tendrán la consideración de copias auténticas, a los efectos de lo previsto en el artículo 46 de la Ley 30/1992.

■ ■ **Artículo 39. Acceso de los interesados a la información sobre el estado de la tramitación del procedimiento**

1. La persona interesada o representante acreditado podrá solicitar y obtener información sobre el estado de la tramitación de los procedimientos administrativos gestionados por medios electrónicos, de acuerdo con lo dispuesto en la Ley 30/1992, de las siguientes formas:
 - a. Presencialmente.
 - b. Telefónicamente.
 - c. Mediante el sistema electrónico empleado para presentar la solicitud, u otro establecido a tal efecto, con las debidas garantías de seguridad y confidencialidad.
2. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con breve indicación sobre su contenido, fecha en la que fueron dictados y persona responsable de cada estado.
3. El Ayuntamiento podrá remitir al interesado avisos sobre el estado de la tramitación, a las direcciones electrónicas de contacto indicadas por el mismo o utilizando los canales que progresivamente se vayan implantando o aquel que el Ayuntamiento estime oportuno en cada momento.

4. En los procedimientos que no hayan sido íntegramente tramitados por medios electrónicos, se habilitarán 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 40. Terminación de los procedimientos por medios electrónicos**

1. De conformidad con lo previsto en el artículo 45.3 de la Ley 30/1992, los procedimientos que se tramiten y se acaben en soporte electrónico garantizarán la identidad y el ejercicio del órgano competente mediante el empleo de alguno de los instrumentos previstos en esta Ordenanza.
2. El acto o resolución que ponga fin a un procedimiento electrónico cumplirá con los requisitos previstos en el artículo 89 de la Ley 30/1992 e irá acompañado de la firma electrónica reconocida del órgano administrativo competente para dictar el acto o resolución.
3. Podrán adoptarse y notificarse resoluciones de forma automatizada en aquellos procedimientos en los que así esté previsto y con los requisitos establecidos en esta Ordenanza.

■ ■ **Artículo 41. Actuación administrativa automatizada**

Los actos administrativos de las entidades integradas en el Ayuntamiento se podrán dictar de forma automatizada, siempre y cuando se dé cumplimiento a los requisitos establecidos para los actos administrativos en la normativa administrativa aplicable y en esta Ordenanza.

■ **Capítulo 10º. Servicio telemático de pago**

■ ■ **Artículo 42. Servicio Telemático de Pagos**

1. El Ayuntamiento y sus organismos públicos habilitarán sistemas electrónicos de pago que permitan a los ciudadanos realizar telemáticamente el ingreso de tributos, sanciones, multas, recargos u otras cantidades, previa liquidación en los casos necesarios. Para ello el Ayuntamiento podrá valerse de pasarelas de pago electrónico habilitadas por otras Administraciones Públicas, que permitan intercambiar datos online con determinadas entidades financieras de forma segura y confidencial, incorporando con ello el pago online en cualquier punto de una tramitación telemática.
2. Se admitirá la presentación, por medios electrónicos, de facturas emitidas por terceros respecto de servicios que les hayan sido prestados, cuando les conste la autenticidad del emisor y del documento y cumpla las demás condiciones establecidas por la normativa correspondiente. Si no contase con la veracidad del emisor o del documento, requerirán la misma al emisor para que la acredite por los medios que la Administración estime oportunos.
3. Los pagos podrán realizarse por cualquier medio admitido por el Servicio Telemático de Pagos y por cualquier entidad financiera adherida. En particular, pagos mediante cargo en cuenta bancaria desde una cuenta corriente abierta o mediante una tarjeta de crédito o débito emitida por una de estas entidades.
4. El sistema de pago electrónico que se habilite emitirá el correspondiente impreso justificativo del pago realizado.

5. La adhesión de las entidades financieras interesadas a la plataforma de pagos telemáticos utilizado por el Ayuntamiento, se realizará conforme al procedimiento y requisitos técnicos previstos para dicha plataforma. Asimismo, el Ayuntamiento podrá validar sistemas alternativos de pagos telemáticos garantizando en todo momento la seguridad del procedimiento.
6. La realización del pago por medio telemático no exime de las obligaciones formales al interesado en relación con el concepto por el que se haya realizado el pago, en particular las relativas a la conservación de la documentación y la presentación de la documentación exigida en el Registro Municipal.
7. La imposibilidad, por el motivo que fuere, de realizar la transacción por el Sistema Telemático de Pagos, no excusará al obligado del pago dentro de los plazos establecidos en la normativa de los correspondientes tributos, precios públicos y demás ingresos de derecho público.
8. Los plazos de devolución de recibo electrónico serán los mismos que en el caso de pago tradicional.

■ *Disposiciones transitorias*

■ ■ PRIMERA: Reunión virtual de órganos colegiados

Si el ordenamiento jurídico y la tecnología disponible lo permiten, los órganos colegiados del Ayuntamiento podrán constituirse y adoptar acuerdos por medios electrónicos, con respeto a los trámites esenciales establecidos en los artículos 26 y 27.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, de acuerdo con las siguientes especialidades:

- a. Garantizar 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, así como 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.

Según el artículo 69 del Reglamento Orgánico Municipal (ROM) del Ayuntamiento de Leganés, la Junta de Gobierno Local podrá acordar la utilización de medios telemáticos para notificar la convocatoria y orden del día de las sesiones, en los términos que prevea la Ley.

Asimismo el artículo 76 indica que las sesiones del Pleno serán públicas. No obstante, cuando así se acuerde por mayoría absoluta, podrán ser secretos el debate y votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución.

Los representantes de los medios de comunicación deberán tener garantizado el acceso y el espacio para desenvolver su tarea en las debidas condiciones. Se ampliará, cuando se considere necesario, la difusión del desarrollo de las sesiones mediante la instalación de megafonía o circuitos de televisión, la utilización de redes de comunicación tales como Internet y el uso de las reglas de signos.

Las sesiones del Pleno del Ayuntamiento se emitirán por Internet en tiempo real, a través de la Sede Electrónica, como un servicio básico de información a los ciudadanos con el objetivo de favorecer la participación de esta en las actividades municipales. Las grabaciones de dichas sesiones podrán ser consultadas posteriormente por cualquier ciudadano.

Asimismo, las actas de las sesiones celebradas por el pleno del Ayuntamiento, podrán ser consultadas en cualquier momento por los ciudadanos a través de la sede electrónica, siempre que así lo estime oportuno el Secretario General del Ayuntamiento.

■ ■ **SEGUNDA: Contratación administrativa**

El Ayuntamiento adoptará las medidas necesarias para fomentar e implantar progresivamente la contratación por vía electrónica y el uso de la factura electrónica por parte de sus contratistas.

■ ■ **TERCERA. Incorporación de trámites y procedimientos actuales**

Los trámites y procedimientos disponibles que actualmente se pueden tramitar electrónicamente, se considerarán incorporados a la tramitación por vía electrónica y se deberán incluir en el catálogo de trámites y procedimientos electrónicos del Ayuntamiento de Leganés desde el momento de entrada en vigor de esta Ordenanza.

■ ■ **CUARTA. Procedimientos en curso**

1. Esta Ordenanza no se aplicará a los procedimientos iniciados con anterioridad a su entrada en vigor.
2. Las Ordenanzas en vigor del Ayuntamiento quedarán obligadas, en el momento de aprobación de la presente Ordenanza, a exigir, en todos los procedimientos y asuntos que sean competencia del Ayuntamiento, la presentación de toda la documentación, solicitudes, escritos o comunicaciones a través del Registro de Entrada del Ayuntamiento por medios electrónicos, en los supuestos previstos en el artículo 27.6 de la Ley 11/2007. Dicha modificación de las Ordenanzas existentes deberá ser publicada en la Sede Electrónica.

■ ■ **QUINTA. Tablón de edictos electrónico**

El tablón de edictos electrónico que regula esta Ordenanza entrará en funcionamiento a lo largo del año 2010 y no superando el plazo de 31 de diciembre de 2010.

■ ■ **SEXTA. Notificación electrónica**

El Ayuntamiento pondrá en marcha la notificación electrónica, para los procedimientos y trámites que lo requieran, en el momento de la aprobación de los decretos de incorporación al catálogo de trámites y procedimientos electrónicos.

■ ■ **SÉPTIMA. Registro Electrónico**

El Ayuntamiento habilitará el acceso al Registro Electrónico, para los procedimientos y trámites que lo requieran, en el momento de la aprobación de los decretos de incorporación en el catálogo de trámites y procedimientos electrónicos. El Registro Electrónico regulado en esta Ordenanza entrará en funcionamiento a lo largo del año 2010, según la Ley 11/2007.

■ ■ **OCTAVA. Archivo electrónico**

1. La Concejalía competente elaborará una propuesta técnica de organización, funcionamiento y puesta en marcha del Archivo Municipal Electrónico, que se deberá emitir en el plazo máximo de un año desde la entrada en vigor de esta Ordenanza.
2. El Ayuntamiento fijará el calendario para que el cumplimiento progresivo de lo previsto en esta disposición, que garantizará su cumplimiento total antes del 1 de Enero de 2011.

■ ■ **NOVENA. Representación electrónica**

La representación electrónica, regulada en diferentes artículos de esta Ordenanza entrará en funcionamiento en momentos diferentes, según el trámite y el procedimiento a realizar, en la medida que lo permitan las disponibilidades presupuestarias de la Corporación, tal y como indica el punto 4 de la Disposición final tercera de la Ley 11/2007.

■ ■ **DÉCIMA. Listado de funcionarios**

El Ayuntamiento mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación de los ciudadanos por funcionario público.

■ *Disposiciones finales*

■ ■ **PRIMERA. Desarrollo y ejecución de la Ordenanza**

De acuerdo con el artículo 124.4, b) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, el Alcalde es el órgano competente para dictar las disposiciones de desarrollo y ejecución de esta Ordenanza que sean necesarias.

■ ■ **SEGUNDA. Seguimiento e implantación de la Ordenanza**

Se encarga a la Delegación de Servicios a la Ciudadanía y Nuevas Tecnologías del Ayuntamiento de Leganés proponer a los órganos de gobierno del Ayuntamiento las acciones de desarrollo, seguimiento y evaluación de la aplicación de esta Ordenanza.

■ ■ **TERCERA. Difusión de la Ordenanza y Formación de los empleados municipales**

El Ayuntamiento difundirá por medios electrónicos esta Ordenanza, una vez que sea aprobada y preparará una edición en soporte electrónico y papel según se determine, para distribuirla entre los ciudadanos, y en particular entre los colectivos y entidades especialmente afectados por su aplicación. El desarrollo de esta Ordenanza preverá las acciones de difusión y de 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 por el personal del Ayuntamiento. El Ayuntamiento promoverá la formación del personal a su servicio en la utilización de medios electrónicos para el desarrollo de las actividades propias de aquella y en concreto en la aplicación y desarrollo de esta ordenanza dentro de un plan de formación continua del departamento de Recursos Humanos del Ayuntamiento de Leganés.

■ ■ CUARTA: Entrada en vigor de la Ordenanza

1. La presente Ordenanza entrará en vigor transcurridos quince días hábiles desde su publicación definitiva en el Boletín Oficial de la Comunidad de Madrid, de acuerdo con lo previsto en los artículos 70.2 y 65.2 de la Ley 7/1985, de 2 de abril, Reguladora del Régimen Local.
2. Según los artículos 196, 198 y 199 del Reglamento Orgánico Municipal del Ayuntamiento de Leganés, la iniciativa para la elaboración de Ordenanzas, Reglamentos y demás disposiciones municipales de carácter general corresponderá al Alcalde, a la Junta de Gobierno Local, a los Concejales, a las Juntas de Distrito y a la iniciativa popular. En el supuesto de que el Pleno del Ayuntamiento delegue en las Comisiones Plenarias la competencia para la aprobación y modificación de las ordenanzas y reglamentos municipales, corresponderá a las Comisiones las competencias atribuidas al Pleno en los Capítulos segundo y tercero del Título III del ROM.
3. Los proyectos de ordenanzas y reglamentos aprobados por la Junta de Gobierno Local, junto con su correspondiente expediente y, en su caso, con la documentación complementaria, se remitirán al Secretario General del Pleno para que, a su vez, los remita al Presidente de la Comisión Plenaria competente.

Corresponde al Pleno la aprobación inicial de las ordenanzas y reglamentos.

■ ■ QUINTA. Regulación de nuevos procedimientos y trámites

A partir de la entrada en vigor de esta Ordenanza, cualquier regulación que se efectúe de nuevos procedimientos y trámites administrativos, o modificación de los existentes, deberá prever la posibilidad de su tramitación por medios electrónicos y se ajustará a las condiciones y requisitos previstos en esta Ordenanza. Su regulación se ajustará al procedimiento de incorporación previsto en el capítulo octavo de la Ordenanza.

■ ■ SEXTA. Adaptación a la normativa municipal

El Ayuntamiento de Leganés se compromete a adaptar la normativa municipal a las previsiones de esta Ordenanza.

■ ANEXO I. *Definiciones*

A los efectos de la presente Ordenanza, se entenderá por:

1. **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.
2. **Autenticación o Identificación Electrónica:** Un conjunto de datos en forma electrónica que, consignados junto a otros o asociados con ellos, pueden ser utilizados como medio para acreditar la identidad de la persona usuaria.
3. **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.)

4. **Certificado electrónico:** Según el Art. 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”.
5. **Ciudadanía:** Cualquier persona física, persona jurídica y ente sin personalidad que se relacione, o sea susceptible de relacionarse con las Administraciones Públicas.
6. **Dominio Web:** Una serie de caracteres que identifican unívocamente un servidor, un sitio o un recurso en Internet y que permiten acceder a él.
7. **Documento electrónico:** Entidad identificada y estructurada producida por medios electrónicos, informáticos y telemáticos que puede ser almacenada, editada, percibida, extraída o intercambiada entre sistemas de tratamiento de la información o usuarios.
8. **Documento electrónico público:** Documento que incluye identificación electrónica compuesta por los datos recogidos en un certificado de firma electrónica acreditado por el Ayuntamiento en sus políticas de validación
9. **Firma Electrónica:** Según el art. 3 de la Ley 59/2003 de 19 de diciembre, de Firma Electrónica, “Conjunto de datos en forma electrónica, consignados junto a otros asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”.
10. **Firma electrónica avanzada:** Según el Art. 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”.
11. **Firma Electrónica reconocida:** Según el Art. 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”.
12. **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.
13. **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 móvil u otras.
14. **Sede Electrónica:** Direcciones electrónicas cuya gestión y administración corresponde a un órgano o entidad administrativa en el ejercicio de sus competencias.
15. **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.

■ ANEXO II. *Trámites y gestiones municipales disponibles en la sede electrónica*

A partir de la fecha de entrada en vigor oficialmente de esta Ordenanza, y sin perjuicio de la progresiva implantación electrónica de los restantes trámites y procedimientos, el Ayuntamiento pone a disposición de los ciudadanos el acceso electrónico al siguiente listado de trámites y gestiones administrativas a través de la **Oficina Virtual**:

Existirá un sistema de validación de documentos que permite garantizar la validez de los documentos generados a través de la **Oficina Virtual**.

- Solicitudes y trámites privados (con necesidad de certificado digital)
- Solicitudes y trámites públicos (sin necesidad de certificado digital)

Otra plataforma informática accesible a través del portal Web es la del **010 Digital Información Ciudadana**. Mediante un motor de búsqueda, el usuario o usuaria dispondrá de información actualizada referente al término municipal de Leganés.

La información que se ofrece se estructura en tres bloques:

- Fichas: Información sobre negocios, transporte público y servicios del Ayuntamiento entre otros (direcciones, teléfonos, horarios, página Web).
- Trámites: Descripción detallada de la documentación necesaria y pasos a seguir para facilitar los trámites a realizar con el Ayuntamiento y otros servicios públicos.
- Guía ciudadana: Búsqueda por dirección de fichas de información general y localización en mapa.

Conforme al marco de calidad total aprobado en el Pleno del Ayuntamiento, se busca fomentar la participación ciudadana y el compromiso firme de la institución municipal y de todos los trabajadores del Ayuntamiento en la mejora continua del nivel de calidad de los servicios prestados. Por ello se ofrece el servicio **ASR (Avisos, Sugerencias y Reclamaciones)** a través de la Sede Electrónica.

El **TABLON ELECTRONICO**, integrado en la Sede Electrónica del Ayuntamiento, es un canal de información con la Ciudadanía que permite la publicación de todos aquellos actos y comunicaciones que, por disposición legal o reglamentaria, deban divulgarse en el Tablón de Anuncios. Facilita el acceso a la información, permitiendo la búsqueda de información de forma rápida y sencilla.

La **Web DEJÓVENES EMPLEO** que también se integra en la Web municipal facilita el proceso de búsqueda de empleo. Los contenidos han sido elaborados basándose en el punto de vista de los jóvenes, por lo que son ellos los encargados de presentar y guiar al usuario o usuaria a través del proceso. Dispone de ayuda interactiva. El Centro de Información Dejóvenes posibilita la utilización de forma gratuita de todos los servicios de información y comunicación de Internet para todos los jóvenes y/o estudiantes con edades comprendidas entre 14 y 35 años, previa solicitud de un carné.

A continuación otros servicios online que ofrece la **Sede Electrónica**:

TRÁMITES ON LINE	
<ul style="list-style-type: none"> - Consultas online - Quejas y sugerencias - Formularios y encuestas online - Citas online (Asesoría jurídica, etc.) - Pagos online / autoliquidaciones online - Registro Electrónico - Tablón de Anuncios Electrónico - Validar documentos - Servicio SMS Leganés - RSS - Servicio de traducción para sordos - Acceso, rectificación y control de datos de carácter personal 	<ul style="list-style-type: none"> - Notificaciones de interés al 010 (cortes por obras, entradas agotadas para eventos, etc.) - Venta de entradas - Inscripción a bolsa de empleo - Alta de ofertas de empleo - Tu opinión nos interesa - Solicitud de tarjetas EnBici - Descarga de publicaciones municipales de utilidad pública - Plataforma de blog: www.cuadernosciudadanos.net - Suscripción boletines electrónicos: DeJóvenes, de Medio Ambiente, El Mogollón, etc.

INFORMACIÓN ON LINE	
<ul style="list-style-type: none"> - Organización municipal - Relación de certificados electrónicos admitidos - Resultado de campeonatos y actividades deportivas - Plenos online y otros eventos - Trámites online - Trámites y gestiones por temas (pendiente) - Catálogo y repositorio telefónico - Guía Ciudadana (datos georeferenciados) - Últimos días para (fin de eventos, campañas, convocatorias, etc.) - Publicación de plicas (Portal de contratación) - Agenda electrónica de eventos. - Información ambiental (ozono, polen, etc.) 	<ul style="list-style-type: none"> - Visitas virtuales - Información de tráfico - Agenda electrónica por temas. - Directorio de empresas. - Aviso de obras y proyectos en vía pública por barrios. - Canal Youtube/Flickr/Facebook/Twitter - Consulta de publicaciones municipales de utilidad pública - Consulta de fondos bibliotecas municipales. - Farmacias de guardia - Directorio de entidades ciudadanas - Publicación de calificaciones - Tablón de edictos electrónico

Cualquier nuevo servicio a incorporar a la sede electrónica que hará por Decreto de Alcaldía y sin necesidad expresa de modificar esta ordenanza.

Sede Electrónica: <https://www.leganes.org>

9.2. Ayuntamiento de Rivas-Vaciamadrid



- *Ordenanza Reguladora de la Administración Electrónica y del Registro Electrónico del Ayuntamiento de Rivas Vaciamadrid*
- **Regulación del uso de las TIC en las relaciones jurídico-administrativas entre los ciudadanos y la Administración municipal**

SUMARIO

EXPOSICIÓN DE MOTIVOS

CAPÍTULO 1º. Disposiciones generales

- Artículo 1. Objeto
- Artículo 2. Ámbito de aplicación
- Artículo 3. La Sede Electrónica
- Artículo 4. Finalidades
- Artículo 5. Cumplimiento y regulación de la E-administración
- Artículo 6. Definiciones

CAPÍTULO 2º. Principios generales

- Artículo 7. Principios generales

CAPÍTULO 3º. Derechos y deberes

- Artículo 8. Derechos de los ciudadanos en el marco de la Administración Electrónica
- Artículo 9. Deberes de los ciudadanos en el marco de las relaciones administrativas establecidas a través de medios electrónicos

CAPÍTULO 4º. Normas de identificación electrónica

- Artículo 10. Normas de identificación, de autenticación y de firma electrónica de los órganos administrativos
- Artículo 11. Normas de identificación, de autenticación y de firma electrónica de los interesados

CAPÍTULO 5º. La difusión de la información administrativa por medios electrónicos

- Artículo 12. Información sobre la organización y los servicios de interés general
- Artículo 13. Información administrativa
- Artículo 14. Calidad y seguridad en la web municipal
- Artículo 15. Tablón de edictos electrónico
- Artículo 16. Publicación oficial

CAPÍTULO 6º. El procedimiento administrativo electrónico

- Artículo 18. Trámites y procedimientos a los que es aplicable la tramitación electrónica

Artículo 19. Iniciación del procedimiento administrativo

Artículo 20. Representación

Artículo 21. Tramitación del procedimiento administrativo

Artículo 22. Continuación del procedimiento administrativo electrónico por medios tradicionales

Artículo 23. Acceso del interesado a la información sobre el estado de la tramitación del procedimiento

Artículo 24. Expediente electrónico

Artículo 25. Terminación de los procedimientos por medios electrónicos

Artículo 26. La notificación telemática de los actos administrativos

Artículo 27. Documentos y certificados administrativos electrónicos

CAPÍTULO 7º. Registro, archivo y acceso a los documentos electrónicos

Artículo 28. Registro Electrónico de entrada y salida de documentos

Artículo 29. Gestión de los documentos electrónicos

Artículo 30. El archivo electrónico del Ayuntamiento de Rivas Vaciamadrid

Artículo 31. Normas sobre el archivo de los documentos

Artículo 32. Responsabilidad

CAPÍTULO 8º. Servicio telemático de pagos

Artículo 33. Servicio Telemático de Pagos

Artículo 34. Procedimiento del Servicio Telemático de Pago

DISPOSICIONES TRANSITORIAS

DISPOSICIONES FINALES

ANEXO I. Trámites y gestiones municipales disponibles actualmente a través del portal del Ayuntamiento de Rivas Vaciamadrid, www.rivas-vaciamadrid.org

ANEXO II. Características de las aplicaciones informáticas de registro y tramitación electrónica utilizadas por el Ayuntamiento de Rivas Vaciamadrid

ANEXO III. Normas para el suministro de cartografía de proyectos y obras y de digitalización

■ Exposición de motivos

- I. Las tecnologías de la información y las comunicaciones (TIC) están transformando profundamente la manera en la que actualmente se desarrolla la actividad de las administraciones públicas, y en especial en lo relativo a sus relaciones con la ciudadanía. Está emergiendo un nuevo entorno que se denomina Sociedad de la Información y el Conocimiento en el que la implantación paulatina de la administración electrónica en todos los niveles administrativos es imparable.

Es responsabilidad de la administración local, en lo que a sus ciudadanos se refiere, generar confianza y seguridad en la utilización de las tramitaciones electrónicas, poniendo a su servicio los avances tecnológicos posibles. En definitiva, es responsabilidad de la administración acortar el camino entre la gestión presencial y la electrónica, así como emprender acciones encaminadas a reducir la barrera que distancia al ciudadano de la administración en general y de la administración local en particular.

Recientemente ha sido aprobada la Ley 11/2007, de 22 de junio, “de acceso electrónico de los ciudadanos a los Servicios Públicos”, de carácter básico en la mayoría de sus artículos y, por consiguiente, de aplicación a todas las administraciones públicas, incluidas las locales. La propia exposición de motivos de esta Ley, refiriéndose al desarrollo de la administración electrónica, califica el cambio que se pretende como el “paso del podrán al deberán”.

El Ayuntamiento de Rivas Vaciamadrid, reconociendo los profundos cambios que está produciendo la incorporación de las TIC en la vida cotidiana de las personas, y en aras al cumplimiento de los objetivos y principios establecidos en la Ley 11/2007, considera necesaria y adecuada una Ordenanza municipal que inicie el desarrollo en el ámbito municipal de los aspectos básicos recogidos en la nueva legislación y que establezca un conjunto de trámites electrónicos que incorporan el registro electrónico como soporte a la presentación de documentos y solicitudes.

Para potenciar el uso más intenso de las tecnologías en las relaciones de los ciudadanos y las empresas con el Ayuntamiento y facilitar el aprovechamiento de sus beneficios, es preciso que éste se dote de un instrumento normativo que determine los derechos y los deberes de los ciudadanos, que regule las condiciones, las garantías y los efectos jurídicos de la utilización de los medios electrónicos en las relaciones con los ciudadanos y que establezca los principios generales de actuación de la Administración Municipal, en especial en el proceso de incorporación a la administración electrónica de los trámites y los procedimientos administrativos. La norma debe dar plena seguridad jurídica, agilidad y eficacia, a la actuación que han hecho y hacen todos los servicios municipales para facilitar, a través de Internet y de los canales telemáticos en general, servicios de información, consulta, tramitación y participación.

Esta Ordenanza constituye un paso adelante más en la implantación paulatina de una verdadera Administración electrónica, que ha de ser, sobre todo, accesible, sencilla, útil, cómoda, ágil, segura, confidencial y adaptada a los nuevos cambios. En su virtud se crea el Registro Electrónico, que va a permitir a la ciudadanía presentar solicitudes y escritos en el registro de la institución por vía electrónica.

La presente Ordenanza debe preservar y potenciar los elementos propios del modelo de desarrollo de la Administración Electrónica en Rivas Vaciamadrid: la orientación de servicio al ciudadano; la agilidad y descentralización en la gestión del medio; la integración con las bases de datos y las aplicaciones corporativas; la plena utilización del potencial de la tecnología; y la ambición de alcanzar un nivel muy elevado de aceptación y de utilización por parte de la ciudadanía.

La Ordenanza debe adecuarse a la realidad de la sociedad, de la organización municipal y de la disponibilidad y madurez de las tecnologías.

II. La presente Ordenanza está en armonía con la dirección y las pretensiones generales del ordenamiento jurídico vigente en la actualidad.

Desde un punto de vista general, el fundamento jurídico concreto de sus disposiciones debe encontrarse, por una parte, directamente en el mandato que impone a las administraciones el artículo 103.1 de la Constitución, que vincula la legitimidad en el ejercicio de las potestades administrativas a los principios de servicio objetivo del interés general. Y, por otra, en los principios definidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, en el ámbito local, en el artículo 6 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, de eficiencia, servicio a los ciudadanos, eficacia, coordinación, transparencia y participación.

Desde un punto de vista más concreto, la Ley 30/1992 reguló la incorporación de las técnicas electrónicas, informáticas y telemáticas al desarrollo de las actividades de la Administración y en el ejercicio de sus competencias, así como la informatización de sus registros y archivos. Posteriormente, la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, trató de potenciar el uso de medios electrónicos, informáticos y telemáticos por la Administración, modificando la Ley 30/1992 en el sentido de habilitar la creación de registros telemáticos que facilitaran e impulsaran las comunicaciones telemáticas, dotando así mismo de cobertura legal al régimen jurídico de las notificaciones telemáticas.

La Ley 11/2007 trata de crear un marco jurídico que facilite la utilización de medios electrónicos en las relaciones entre la Administración y los ciudadanos.

Finalmente, el Reglamento Orgánico Municipal del Ayuntamiento de Rivas Vaciamadrid, publicado en el Boletín Oficial de la Comunidad de Madrid de 8 de mayo de 2009, en su **Capítulo III** “Resoluciones, comunicaciones y notificaciones” del **Título I** “El alcalde/la alcaldesa”, hace referencia expresa a la administración electrónica.

III. El Ayuntamiento de Rivas Vaciamadrid, en ejercicio de su potestad autoorganizativa, dicta esta Ordenanza con el objeto, expuesto en el capítulo primero, de regular la utilización de las TIC en las relaciones jurídico-administrativas entre los ciudadanos y la Administración Municipal. El capítulo segundo establece los principios generales de actuación de la Administración Municipal en el ámbito de la Administración Electrónica. El capítulo tercero reconoce los derechos y los deberes de los ciudadanos y, por lo tanto, las obligaciones y las garantías de la Administración Municipal en lo que concierne al uso de las TIC en las relaciones administrativas. Se muestra asimismo una lista de los deberes o las condiciones del uso responsable de la Administración Electrónica por parte de los ciudadanos.

El capítulo cuarto se dedica a los sistemas de identificación en los diferentes tipos de relaciones entre los ciudadanos y el Ayuntamiento. Con el capítulo quinto se consolida una política que garantiza la máxima difusión, por medios electrónicos, de la información de que disponga el Ayuntamiento. En el capítulo sexto se regulan las diferentes fases o trámites del procedimiento administrativo electrónico general, los certificados y las compulsas. En el capítulo séptimo se regula el régimen de funcionamiento del Registro Electrónico, el archivo electrónico de documentos y las condiciones de acceso de los ciudadanos a los registros y archivos electrónicos. En el Capítulo octavo se regula el Servicio Telemático de Pago.

Las disposiciones contenidas en el Régimen Transitorio deben permitir la implantación decidida, progresiva y eficiente de la administración electrónica en todo el Ayuntamiento. De manera inmediata, se configura el catálogo de trámites y procedimientos y se incorporan a la tramitación por vía electrónica los que ya están disponibles.

Las disposiciones finales autorizan a dictar las disposiciones que sean necesarias para el desarrollo de la Ordenanza y, en particular, el compromiso de adaptar a ella el resto de la normativa municipal y la difusión proactiva de la norma, tanto a través de medios electrónicos como en soporte papel.

■ **Capítulo 1º. Disposiciones generales**

■ ■ **Artículo 1. Objeto**

La presente Ordenanza; en virtud del reconocimiento al derecho de los ciudadanos a relacionarse por medios electrónicos con las Administraciones Públicas que se consagra en el Art. 1 de la Ley 11/2007; fija las reglas generales para la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones con los ciudadanos, en el ámbito de la Administración Municipal de Rivas Vaciamadrid, con la finalidad de garantizar los derechos de los ciudadanos, un tratamiento común y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

■ ■ **Artículo 2. Ámbito de aplicación**

1. La Ordenanza será de aplicación a las entidades siguientes:
 - a. Los órganos administrativos del Ayuntamiento
 - b. Los entes de derecho público y de derecho privado vinculados a él.
 - c. Las sociedades y las entidades concesionarias de servicios públicos municipales, cuando así lo disponga el título concesional o lo aprueben sus órganos de gobierno, en sus relaciones con el Ayuntamiento y con los ciudadanos, en el marco de la prestación de servicios públicos municipales y en el ejercicio de potestades administrativas de su competencia.
2. La Ordenanza será aplicable a los ciudadanos, entendiéndose como tales a las personas físicas y jurídicas, cuando utilicen medios electrónicos en sus relaciones con el Ayuntamiento y con el resto de las entidades referidas en el apartado anterior.

■ ■ **Artículo 3. La Sede Electrónica**

1. El punto de acceso general del Ayuntamiento de Rivas Vaciamadrid es la sede electrónica, que, en este ámbito, facilita el acceso a la totalidad de los servicios, procedimientos e informaciones accesibles.
 - a. El acceso se organizará atendiendo a criterios que permitan a los ciudadanos identificar de forma fácil e intuitiva los servicios a los que deseen acceder. Para ello la información y el acceso se clasificará, al menos, en base a los colectivos destinatarios de los servicios, a los ámbitos materiales de la actividad administrativa o a las circunstancias personales o eventos vitales relacionados con los servicios.
 - b. El Punto de acceso general será gestionado por la Concejalía competente en materia de innovación tecnológica y modernización administrativa, con la participación de la restantes Concejalías municipales para garantizar la completa y exacta incorporación de la información y accesos publicados en éste.
2. La sede electrónica de la Administración Municipal se establece en la dirección de Internet: www.rivas-vaciamadrid.org.
3. La Junta de Gobierno Local podrá acordar la modificación de la sede electrónica.

4. Se podrán crear, previo acuerdo de la Junta de Gobierno Local, una o varias sedes electrónicas derivadas de la sede electrónica establecida en el punto 2. 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.
5. La sede y las subsedes electrónicas dispondrán del siguiente contenido:
 - 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, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relacionada con propiedad intelectual.
 - c. Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.
 - d. Relación de sistemas de firma electrónica que, entre los autorizados en esta Ordenanza, sean admitidos o utilizados en la sede.
6. La sede electrónica proporcionará el acceso a las normas y reglamentos del Registro Electrónico y a sus aplicaciones gestoras o tramitadoras.
7. La sede electrónica dispondrá de los siguientes servicios:
 - a. Relación de los servicios disponibles en la sede electrónica y, en su caso, la carta de servicios.
 - b. Relación de los medios electrónicos a los que se refiere el artículo 27.4 de la Ley 11/2007.
 - c. Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.
 - d. Acceso, en su caso, al estado de tramitación del expediente en los términos establecidos en el presente reglamento.
 - e. 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.
 - f. Indicación de la fecha y hora oficial a los efectos previstos en el artículo 26.1 de la Ley 11/2007, así como el calendario oficial.
8. 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 y en esta Ordenanza.
9. Las decisiones relativas al alojamiento en servidores y adquisición de dominios y subdominios relacionadas con todas las sedes y subsedes electrónicas del Ayuntamiento serán competencia exclusiva de la Concejalía competente en materia de sistemas informáticos.

■ ■ Artículo 4. Finalidades

Son fines de la presente Ordenanza:

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, con las debidas garantías legales, oportunidades de participación y transparencia.
7. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.

■ ■ Artículo 5. Cumplimiento y regulación de la E-administración

La Administración Municipal velará por el cumplimiento de lo contenido en la presente Ordenanza, en el marco de lo previsto en la normativa aplicable y en las previsiones de este Reglamento.

Con tal objeto, la Concejalía competente en materia de innovación tecnológica y modernización administrativa elaborará informe preceptivo y vinculante en cuantas disposiciones generales y procedimientos administrativos en general se implanten para adaptarlos a los requisitos técnicos de la Administración Electrónica y a las características tecnológicas del Ayuntamiento.

■ ■ Artículo 6. Definiciones

A los efectos de la presente Ordenanza, se entenderá por:

1. **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.
2. **Aplicación Informática:** Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el recurso a un sistema de tratamiento de la información.
3. **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.

4. **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.)
5. **Certificado Electrónico:** Según el Art. 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”.
6. **Certificado Electrónico reconocido:** Según el Art. 11 de la Ley 59/2003: “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”.
7. **Dirección Electrónica:** Una serie de caracteres que identifican unívocamente un servidor, un sitio o un recurso en Internet y que permiten acceder a él.
8. **Documento Electrónico:** Entidad identificada y estructurada producida por medios electrónicos, informáticos y telemáticos que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, percibida, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada.
9. **Estándar Abierto:** Aquel que reúne 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.
10. **Firma Electrónica:** Según el artículo 3 de la Ley 59/2003, “Conjunto de datos en forma electrónica, consignados junto a otros asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”.
11. **Firma Electrónica avanzada:** Según el Art. 3 de la Ley 59/2003, “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”.
12. **Firma Electrónica reconocida:** Según el Art. 3 de la Ley 59/2003, “firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”.
13. **Formulario Electrónico:** Un documento electrónico estructurado, con campos de información predefinidos, que sirve de soporte para la carga de las solicitudes, escritos y comunicaciones referidas a trámites o procedimientos administrativos susceptibles de recepción y remisión mediante Registro Electrónico y que se encuentra disponible a tal efecto en el portal corporativo del Ayuntamiento.
14. **Identificación Electrónica o Autenticación:** Un conjunto de datos en forma electrónica que, consignados junto a otros o asociados con ellos, pueden ser utilizados como medio para acreditar la identidad de la persona usuaria.

15. **Identificación Electrónica con certificado:** Una identificación electrónica compuesta por los datos recogidos en un certificado de firma electrónica acreditado por el Ayuntamiento en sus políticas de validación.
16. **Identificación Electrónica con contraseña:** Una identificación electrónica compuesta por un código de usuario/a y una contraseña previamente facilitados por el Ayuntamiento.
17. **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.
18. **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 móvil u otras.
19. **Punto de Acceso Electrónico:** Conjunto de páginas WEB agrupadas en un dominio de Internet cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios dirigidos a resolver necesidades específicas de un grupo de personas o el acceso a la información y servicios de una institución pública.
20. **Sede Electrónica:** direcciones electrónicas cuya gestión y administración corresponde a un órgano o entidad administrativa en el ejercicio de sus competencias.
21. **Sistema Informático:** Un programa o conjunto de programas informáticos que tienen por objeto el tratamiento electrónico de información.
22. **Soporte Informático:** Objeto sobre el que es posible grabar y recuperar datos o documentos electrónicos.

■ Capítulo 2º. Principios generales

■ ■ Artículo 7. Principios generales

El Ayuntamiento de Rivas Vaciamadrid asume los siguientes principios informadores de la implantación de la administración electrónica:

1. **Principio de servicio al ciudadano:** El Ayuntamiento impulsará la incorporación de información, trámites y procedimientos a la Administración Electrónica para posibilitar la consecución más eficaz de los principios constitucionales de transparencia administrativa y servicio al ciudadano.
2. **Principio de respeto a la Protección de Datos de carácter personal.** En los términos previstos en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en las demás Leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como en la "Ordenanza Municipal de creación, modificación y supresión de ficheros de datos de carácter personal del Ayuntamiento de Rivas Vaciamadrid y de aplicación de procedimientos de seguridad" y en los derechos al honor y la intimidad personal.
3. **Principio de no discriminación.** El uso de los medios electrónicos no puede comportar restricciones o discriminación alguna de los municipios y ciudadanos en sus relaciones con la administración, 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.

4. **Principio de accesibilidad a la información y a los servicios por medios electrónicos.** Establecidos en la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensiva, 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.
5. **Principio de legalidad.** En cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas.
6. **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.
7. **Principio de proporcionalidad.** Sólo se exigirán garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.
8. **Principio de impulso de los medios electrónicos para una mayor eficacia y eficiencia de la actuación pública.** Como entidad pública, el Ayuntamiento debe impulsar el uso de los medios electrónicos en sus relaciones internas y externas, habiendo de aplicar los medios personales y materiales pertinentes para su efectiva realidad.
9. **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.
10. **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 se utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.
11. **Principio de simplificación administrativa.** El proceso de incorporación de los medios electrónicos al procedimiento administrativo debe conllevar el análisis del proceso mismo, la reconducción a categorías generales, el reconocimiento legal de determinados automatismos electrónicos, en su caso, y la eliminación de trámites o actuaciones no relevantes, de conformidad con la normativa de aplicación.
12. **Principio de publicidad y transparencia.** El uso de medios electrónicos ha de facilitar el cumplimiento de las obligaciones legales de máxima difusión, publicidad y transparencia de las actuaciones administrativas.
13. **Principio de actualización:** Los diferentes órganos de la Administración Municipal mantendrán actualizada la información administrativa que sea accesible a través de canales electrónicos.
14. **Principio de participación.** El uso de medios electrónicos en la administración se ha de poner al servicio de una mejor y más activa participación de los vecinos en la gestión y gobierno de sus intereses colectivos.
15. **Principio de colaboración y cooperación entre las Administraciones Públicas.** La simplificación administrativa al servicio de los ciudadanos requiere el uso de los medios telemáticos como canal básico para las relaciones jurídicas interadministrativas. En este contexto se ha de garantizar tanto la plena interoperabilidad como,

en su caso, la integración para posibilitar la prestación conjunta de servicios a los ciudadanos, con reconocimiento mutuo de los documentos y certificaciones electrónicas. 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 Ley 11/2007.

16. **Principio de Sede Electrónica.** Son atributos de la sede electrónica la accesibilidad y usabilidad, así como la asociación de un régimen de identificación segura y de responsabilidad del titular respecto de la integridad, veracidad y actualización de las informaciones, servicios y transacciones a las que pueda accederse.

■ Capítulo 3º. *Derechos y deberes*

■ ■ Artículo 8. **Derechos de los ciudadanos en el marco de la Administración Electrónica**

1. En el marco del acceso y la utilización de la Administración Electrónica Municipal, los ciudadanos tienen los siguientes derechos:
 - a. **Derecho a dirigirse a la Administración Municipal a través de medios electrónicos, presentar documentos, realizar trámites y procedimientos y, en general, ejercer los derechos y las facultades que les reconoce el ordenamiento jurídico administrativo, con total validez y seguridad.**
 - b. **Derecho a exigir de la Administración Municipal que se dirija a ellos a través de estos medios y obtener documentos a través de formatos electrónicos.**
 - c. **Derecho a no presentar datos y documentos que se encuentren en poder de la Administración Municipal,** las cuáles 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.
 - d. **Derecho a disfrutar de contenidos electrónicos de calidad, accesibles, transparentes y comprensibles.**
 - e. **Derecho 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.
 - f. **Derecho a obtener copias electrónicas de los documentos electrónicos que formen parte del procedimiento en los que tenga condición de interesado.**
 - g. **Derecho a participar en los procesos de toma de decisiones y en la mejora de la gestión municipal a través de medios electrónicos, y a recibir respuesta a las peticiones y consultas formuladas.**
 - h. **Derecho a acceder a la administración electrónica y utilizarla independientemente de las disminuciones físicas o psíquicas.**
 - i. **Derecho a disponer de formación y ayuda en la utilización de la Administración Electrónica.**
 - j. **Derecho a acceder a la Administración Electrónica y utilizarla independientemente de las herramientas tecnológicas utilizadas** y con plena libertad para la elección del canal o medio de los que resulten disponibles en cada momento.

- k. **Derecho a utilizar los sistemas de firma electrónica del DNI y de Firma Electrónica avanzada para cualquier trámite con esta Administración.**
 - l. **Derecho a la confidencialidad y protección de sus datos personales y al resto de los derechos que le concede la normativa de protección de datos**, en especial el derecho a que la información personal entregada no pueda ser destinada a ninguna otra finalidad.
 - m. **Derecho a la privacidad y seguridad de sus comunicaciones con la Administración Municipal y de aquellas comunicaciones que pueda hacer el Ayuntamiento en las que consten los datos de los ciudadanos.**
2. Derecho 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. El ejercicio de estos derechos se llevará a cabo según lo previsto en la normativa aplicable y en las previsiones de esta Ordenanza.

■ ■ **Artículo 9. Deberes de los ciudadanos en el marco de las relaciones administrativas establecidas a través de medios electrónicos**

En el marco de la utilización de los medios electrónicos en la actividad administrativa y en sus relaciones con la Administración Municipal, y para garantizar el buen funcionamiento y gestión de la información, las comunicaciones, los procesos y las aplicaciones de la Administración Electrónica, la actuación de los ciudadanos debe estar presidida por los siguientes deberes:

- a. **Deber de utilizar de buena fe los servicios y procedimientos** de la Administración Electrónica.
- b. **Deber de facilitar a la Administración Municipal**, en el ámbito de la Administración Electrónica, **información veraz, completa y precisa, adecuada a los fines para los que se solicita.**
- c. **Deber de identificarse por medios electrónicos** en las relaciones administrativas con la Administración Municipal, cuando así se requiera.
- d. **Deber de custodiar los elementos identificativos personales e intransferibles utilizados** en las relaciones administrativas por medios electrónicos con la Administración Municipal.
- e. **Deber de respetar el derecho a la privacidad, confidencialidad y seguridad y el resto de los derechos en materia de protección de datos.**

■ **Capítulo 4º. Normas de identificación electrónica**

■ ■ **Artículo 10. Normas de identificación, de autenticación y de firma electrónica de los órganos administrativos**

1. De acuerdo con el artículo 13 de la Ley 11/2007, en relación con el artículo 3 de la Ley 59/2003, la identificación de los trabajadores públicos y de los órganos administrativos se hará mediante firma electrónica reconocida.
2. Los actos administrativos de las entidades integradas en la Administración Municipal se podrán dictar de forma automatizada, siempre y cuando se de cumplimiento a los requisitos establecidos para los actos administrativos en la normativa administrativa aplicable y en esta Ordenanza.

■ ■ Artículo 11. Normas de identificación, de autenticación y de firma electrónica de los interesados

1. La identificación y acreditación de la voluntad de los ciudadanos en las relaciones con la Administración Municipal se podrá producir a través de los siguientes instrumentos o mecanismos:
 - a. Para personas físicas, los certificados electrónicos del DNI electrónico, de acuerdo con la normativa reguladora de dicho documento.
 - b. Para personas físicas, personas jurídicas y entes sin personalidad, otros certificados electrónicos conformes a lo estipulado en la Ley 59/2003, incluyendo la posibilidad de que contengan referencias a otras circunstancias personales o atributos.
 - c. Para órganos administrativos, certificados electrónicos que identificarán al órgano que tenga atribuida la competencia y al titular del mismo.
 - d. Para sistemas automatizados que no precisan intervención personal y directa del titular del órgano administrativo, certificados electrónicos que deberán incluir información sobre la identificación del órgano responsable del trámite y del titular de aquél.
 - e. En general, el uso de claves concertadas en un registro previo como usuario, en los casos y con las limitaciones que establezca la Administración Municipal.
 - f. En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o acreditación de la voluntad del ciudadano mediante alguno de los instrumentos anteriores de los que aquél no disponga, tal identificación o acreditación podrá ser válidamente realizada por los funcionarios públicos de la Administración Municipal que tengan asignada esta función, mediante el uso de certificado electrónico de la Administración Municipal. Para ello, el ciudadano deberá identificarse mediante la exhibición de su DNI y prestar su consentimiento expreso mediante la firma de una copia en papel del formulario o modelo electrónico objeto de la operación, que quedará archivada para su constancia en caso de discrepancia o litigio.
2. El conjunto de certificados y prestadores públicos y privados de servicios de certificación admitidos, con carácter general, por la Administración Municipal, será público y accesible a través de la sede electrónica, incluyendo las características asociadas al tipo de firma electrónica que puede realizarse con cada certificado emitido por cada prestador.
3. La Administración Municipal promoverá la utilización de los medios de identificación electrónica más extendidos en el ámbito social.
4. La Administración Municipal dispondrá de los elementos técnicos y administrativos que permitan la interoperabilidad de los certificados electrónicos emitidos por prestadores de servicios de certificación dependientes o vinculados a una Administración Pública y por aquellos prestadores no dependientes ni vinculados que hayan sido admitidos como válidos para relacionarse con alguna Administración Pública, siempre que la información necesaria de acuerdo con la normativa de firma electrónica se encuentre disponible en condiciones tecnológica y económicamente viables.
5. Será de libre acceso para los ciudadanos, sin necesidad de identificación, la siguiente información:

- a. Información sobre la organización municipal y los servicios de interés general.
 - b. Consultas de disposiciones generales e información normativa.
 - c. Información incluida en el tablón de edictos electrónico.
 - d. Publicaciones oficiales de cualquiera de los órganos y entes de la Administración Municipal.
 - e. Expedientes sometidos a información pública.
 - f. La relación de certificados y prestadores públicos y privados admitidos por la Administración Municipal.
 - g. Cualquier otra información de acceso general.
6. La utilización de cualquiera de los instrumentos de identificación y autenticación recogidos en este artículo será requisito suficiente para identificar y entender acreditada la voluntad de los ciudadanos que presenten escritos en cualquier procedimiento o trámite incorporado a la tramitación por vía electrónica a través del procedimiento previsto en esta Ordenanza.
7. De conformidad con lo dispuesto en el artículo 71 de la Ley 30/1992, la Administración Municipal requerirá de los particulares la enmienda de cualquier defecto formal ocasionado por el incumplimiento de los requisitos de identidad, integridad y autenticidad previstos en este artículo.

■ **Capítulo 5º. *La difusión de la información administrativa por medios electrónicos***

■ ■ **Artículo 12. Información sobre la organización y los servicios de interés general**

1. La Administración Municipal facilitará por medios electrónicos, como mínimo a través de la página web del Ayuntamiento, información sobre:
 - a. Su organización y sus competencias.
 - b. Los servicios que tenga encomendados o asumidos, con la indicación de las prestaciones concretas y la disponibilidad de cada uno de los servicios.
 - c. Los procedimientos administrativos que tramitan, con indicación de los requisitos esenciales y de los plazos de resolución y notificación, así como del sentido del silencio.
 - d. Los datos de localización, como son la dirección postal, el número de teléfono y la dirección de correo electrónico.
 - e. El texto actualizado de esta Ordenanza.
 - f. Los medios electrónicos que los particulares pueden utilizar en ejercicio de su derecho a comunicarse con ellas.
 - g. La relación actualizada de programas y aplicaciones utilizados por la Administración Municipal.
 - h. La relación actualizada de procedimientos, trámites, solicitudes, escritos y comunicaciones susceptibles de presentación y/o tramitación telemática.

2. Se podrá difundir a través de medios electrónicos cualquier otra información relativa a asuntos o cuestiones de interés general para los ciudadanos, incluida la que pueda contribuir a una mejor calidad de vida de los ciudadanos y tenga una especial incidencia social, por ejemplo en los ámbitos de sanidad, salud, cultura, educación, servicios sociales, medio ambiente, transportes, comercio, deportes y tiempo libre.

■ ■ Artículo 13. Información administrativa

La Administración Municipal facilitará a través de medios electrónicos toda la información administrativa que por prescripción legal o resolución judicial se tenga que hacer pública, especificando en la medida de lo posible el órgano administrativo autor del acto o disposición publicados. A modo de ejemplo, la Administración Municipal hará pública la siguiente información:

- a. Los acuerdos de los órganos de gobierno.
- b. Las Ordenanzas municipales.
- c. El presupuesto municipal.
- d. Las figuras de planeamiento urbanístico.
- e. Los anuncios de información pública.
- f. Los procedimientos de contratación administrativa.
- g. Los procedimientos de concesión de subvenciones.
- h. Los procedimientos de selección de personal.
- i. Los impresos y formularios de trámites y procedimientos municipales.

■ ■ Artículo 14. Calidad y seguridad en la web municipal

1. Los servicios de la web municipal estarán operativos las 24 horas del día, todos los días del año, exceptuando casos de fuerza mayor. Cuando por razones técnicas se prevea que la web o algunos de sus servicios pueden no estar operativos, se deberá informar de ello a los usuarios con la máxima antelación posible indicando cuáles son los medios alternativos de consulta disponibles.
2. Se garantizará la seguridad de las páginas web de las entidades incluidas en el ámbito de aplicación de esta Ordenanza, para garantizar la autenticidad e integridad de la información digital que recogen. En particular, los actos administrativos y resoluciones dictados por la Administración Municipal y las comunicaciones con los ciudadanos que se realicen por medios electrónicos deberán cumplir los requisitos de seguridad, integridad y conservación previstos en la Ley 11/2007.

Las medidas de seguridad respetarán el principio de proporcionalidad atendida la naturaleza del trámite o actuación de que se trate.

3. La web municipal cumplirá los estándares de accesibilidad y calidad recomendados para las Administraciones Públicas, y en particular se garantizará que los servicios, informaciones, trámites y procedimientos objeto de esta Ordenanza sean accesibles desde los principales navegadores y sistemas operativos.

4. Las entidades incluidas en el artículo 2 de esta Ordenanza no son responsables en ningún caso de la información que se pueda obtener a través de fuentes externas que no dependan de ellas, ni tampoco de las opiniones que puedan expresar, a través de las páginas web municipales, las personas no vinculadas a dichas entidades.

■ ■ Artículo 15. Tablón de edictos electrónico

1. El tablón de edictos electrónico permitirá el acceso por medios electrónicos a la información que, en virtud de una norma jurídica o resolución judicial, se deba publicar o notificar mediante edictos. El acceso al tablón de edictos electrónico no requerirá ningún mecanismo especial de acreditación de la identidad del ciudadano.
2. El tablón de edictos electrónico se podrá consultar a través de la web municipal, desde terminales instalados en la sede de la Corporación y desde otros puntos de acceso electrónico que se determinen. En todo caso, se garantizará el acceso a todas las personas, así como la ayuda necesaria para lograr una consulta efectiva.
3. El tablón de edictos electrónico dispondrá de los sistemas y mecanismos que garanticen la autenticidad, la integridad y la disponibilidad de su contenido, en los términos previstos en la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos. En especial, a los efectos del cómputo de los plazos que corresponda, se establecerá el mecanismo que garantice la constatación de la fecha y hora de publicación de los edictos.
4. El tablón de edictos electrónico estará disponible las 24 horas del día, todos los días del año, a través de la web municipal, exceptuando casos de fuerza mayor. Cuando por razones técnicas se prevea que el tablón de edictos electrónico puede no estar operativo, se deberá informar de ello a los usuarios con la máxima antelación posible, indicando cuáles son los medios alternativos de consulta del tablón que estén disponibles.

■ ■ Artículo 16. Publicación oficial

La difusión de información y documentación por medios electrónicos no sustituye la publicidad de las disposiciones normativas y los actos que deban ser publicados en un boletín oficial, conforme a las Leyes. A pesar de ello, la difusión de información y documentación por medios electrónicos puede complementar la publicidad realizada en boletines oficiales en soporte papel, en aquellos supuestos en que, por las limitaciones de este medio, no sea obligatorio publicar el contenido completo de las disposiciones o actos objeto de publicación.

■ ■ Artículo 17. Comunicaciones de la Administración Municipal

1. Los órganos de la Administración Municipal, sus organismos públicos vinculados así como las diferentes Concejalías que componen el Ayuntamiento deberán utilizar preferentemente medios electrónicos para comunicarse entre ellos.
2. La Administración Municipal y sus organismos públicos vinculados deberán utilizar preferentemente medios electrónicos para comunicarse con otras Administraciones Públicas.

■ Capitulo 6º. *El procedimiento administrativo electrónico*

■ ■ Artículo 18. Trámites y procedimientos a los que es aplicable la tramitación electrónica

1. Una vez que se apruebe y entre en vigor esta Ordenanza, podrán tramitarse telemáticamente:

- a. Los procedimientos administrativos que se determinen, tanto con respecto al cumplimiento de trámites del procedimiento como la consulta del estado de tramitación y, en aquellos procedimientos que se considere conveniente, la comunicación de avisos de interés dentro del procedimiento.
 - b. Consulta de información de datos municipales por los ciudadanos.
 - c. Comunicaciones de los ciudadanos, en especial los avisos, las quejas, las sugerencias y las peticiones que así se determinen, no incardinables en un procedimiento administrativo.
2. Figuran en el Anexo I de esta Ordenanza relación detallada de los procedimientos, trámites, solicitudes, escritos y comunicaciones que se podrán tramitar telemáticamente a partir de la fecha de su entrada en vigor. Por acuerdo de Junta de Gobierno Local se podrán incluir nuevos trámites y procedimientos, previos los informes que resulten procedentes.
 3. La relación actualizada de procedimientos, trámites, solicitudes, escritos y comunicaciones que se podrán tramitar telemáticamente será accesible a través de la web municipal. Igualmente, la web municipal facilitará información sobre los trámites a seguir en aquellos procedimientos que no se pueden tramitar de forma telemática.
 4. La tramitación de un procedimiento administrativo por medios telemáticos no podrá suponer ninguna merma en el mantenimiento de la integridad de las garantías jurídicas de los particulares ante las Administraciones Públicas establecidas en el Ordenamiento Jurídico y, en particular, en la Ley 30/1992.

■ ■ Artículo 19. Iniciación del procedimiento administrativo

1. Los procedimientos administrativos incorporados a la tramitación por vía electrónica se podrán iniciar a través de medios electrónicos a instancia de parte, mediante la presentación de solicitud, normalizada o no, en el Registro Electrónico regulado en esta Ordenanza.
2. Las solicitudes electrónicas mencionadas en el apartado anterior deberán contener la firma electrónica avanzada del interesado o cualquier otro mecanismo de identificación y de acreditación que establezcan las normas de desarrollo de esta Ordenanza, y todos los demás requisitos establecidos en el artículo 70 de la Ley 30/1992.
3. Los interesados podrán aportar al expediente copias digitalizadas de los documentos que sean necesarios o estimen oportunos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica reconocida. La Administración Municipal podrá en cualquier momento requerir al interesado la exhibición del documento o de la información original o solicitar del correspondiente archivo, el cotejo del contenido con las copias aportadas. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos.
4. 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 interesado verifique la información y, en su caso, la modifique y complete.

■ ■ Artículo 20. Representación

1. Cuando en una solicitud telemática haya más de un interesado, la solicitud deberá estar firmada electrónicamente por todos los interesados, y las actuaciones se seguirán con el que se haya señalado expresamente o, en su defecto, con el interesado que aparezca encabezando la solicitud.
2. Los ciudadanos podrán actuar por medio de representantes en los procedimientos y trámites administrativos que se realicen frente a la Administración Municipal por medios electrónicos, de acuerdo con lo que prevé la legislación general y lo que establece esta Ordenanza. En estos supuestos, la validez de las actuaciones realizadas estará sujeta a la acreditación de la representación.
3. Cualquier persona física con capacidad de obrar puede representar por vía telemática a otras personas, físicas o jurídicas, siempre que acredite la citada representación mediante uno de los siguientes mecanismos alternativos:
 - a. Aportación de apoderamiento suficiente en soporte electrónico original, según las disposiciones vigentes en materia de seguridad jurídica electrónica.
 - b. Inclusión del apoderamiento en el certificado reconocido de firma del representante, de acuerdo con la legislación vigente de firma electrónica.
 - c. Mediante la declaración del apoderamiento por parte del representante y la posterior comprobación de la representación en los registros de la Administración Municipal o de otras administraciones o entidades con las que la Corporación haya firmado un convenio de colaboración.
4. La representación telemática podrá ser específicamente otorgada, a todos los efectos o para procedimientos concretos, presencialmente ante la propia Administración mediante la compulsa electrónica de la documentación acreditativa de la representación, que quedará registrada a los efectos de su certificación.
5. La representación otorgada por vías telemáticas será válida para la tramitación de procedimientos administrativos por vías telemáticas y no telemáticas.
6. Cuando el procedimiento lo permita y así se considere conveniente, la Administración Municipal podrá, en cualquier momento, pedir al apoderado la justificación del apoderamiento y la declaración responsable sobre su vigencia.

■ ■ Artículo 21. Tramitación del procedimiento administrativo

1. Los programas, aplicaciones y sistemas de información que en cada caso se aprueben para la realización por medios electrónicos de los trámites administrativos deberán garantizar el control de los plazos, la constancia de la fecha y hora y la identificación de los responsables de los trámites y actuaciones, además de respetar el orden de tramitación de los expedientes.
2. Cualquier actuación del interesado y los actos administrativos hechos en un procedimiento administrativo tramitado electrónicamente habrán de reunir los requisitos de validez legalmente establecidos con carácter general.
3. Los órganos administrativos velarán especialmente para garantizar el ejercicio a través de medios telemáticos del derecho de los interesados a formular alegaciones en cualquier momento anterior a la propuesta de resolución, en la práctica del trámite de audiencia y en el trámite de información pública cuando procedan.

4. De acuerdo con los principios de simplicidad administrativa e interoperabilidad entre Administraciones, las entidades comprendidas en el ámbito de aplicación de esta Ordenanza promoverán la eliminación de certificados y, en general, de documentos en papel, que serán sustituidos, siempre que sea posible, por certificados y documentos electrónicos o por transmisiones de datos, con plena validez y eficacia siempre que se acredite la identidad, integridad, autenticidad y confidencialidad de los datos mediante los correspondientes certificados de firma electrónica reconocida.

Tanto en el caso de certificados electrónicos y documentos electrónicos como en el de transmisiones de datos, su expedición, tratamiento y efectos se regirán por lo dispuesto en esta Ordenanza, con estricta sujeción a la normativa de protección de datos de carácter personal, así como al resto de la normativa aplicable al procedimiento administrativo.

Para la sustitución de un certificado en papel por la transmisión de los datos correspondientes, el titular de éstos tiene que haber consentido expresamente la realización de la transmisión, de acuerdo con lo que establece la normativa de protección de datos de carácter personal, excepto en los casos previstos en una norma con rango de Ley. Si no presta su consentimiento, el interesado deberá solicitar y aportar el certificado correspondiente.

5. La aportación en papel u otro soporte físico de documentos que estén relacionados con un procedimiento administrativo electrónico, deberá dejar constancia del número o código de registro individualizado correspondiente a aquel procedimiento en el Registro Electrónico.
6. Las entidades comprendidas en el ámbito de aplicación de esta Ordenanza promoverán la sustitución de la aportación de documentos acreditativos del cumplimiento de requisitos por una declaración responsable del interesado que exprese la concurrencia de dichos requisitos y el compromiso de aportar los justificantes, a requerimiento de la Administración.

■ ■ Artículo 22. Continuación del procedimiento administrativo electrónico por medios tradicionales

Cuando un procedimiento iniciado electrónicamente no se pueda tramitar totalmente en soporte electrónico se procederá, por parte del órgano competente a la reproducción en soporte papel de las solicitudes, comunicaciones u otros documentos electrónicos, para poder continuar con la tramitación del expediente, asegurándose en cualquier caso el archivo seguro de los documentos electrónicos originales.

En todo caso, para garantizar la concordancia entre los documentos electrónicos originales y los reproducidos en papel, en toda copia se hará constar la diligencia del funcionario competente que acredite la correspondencia y exactitud con el documento original. Estos documentos tendrán la consideración de copias auténticas, a los efectos de lo previsto en el artículo 46 de la Ley 30/1992.

■ ■ Artículo 23. Acceso del interesado a la información sobre el estado de la tramitación del procedimiento

1. El interesado podrá solicitar y obtener información sobre el estado de la tramitación de los procedimientos administrativos gestionados en su totalidad por medios electrónicos, mediante los siguientes sistemas:
 - a. Presencialmente.
 - b. Mediante el sistema telemático empleado para presentar la solicitud, u otro establecido a tal efecto, con las debidas garantías de seguridad y confidencialidad.

2. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con breve indicación sobre su contenido, así como la fecha en la que fueron dictados.
3. La Administración Municipal podrá remitir al interesado avisos sobre el estado de la tramitación, a las direcciones telemáticas de contacto indicadas por el mismo.
4. En los procedimientos que hayan sido parcialmente tramitados por medios electrónicos, se habilitarán 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 24. 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, pudiendo incluir grabaciones de conversaciones consentidas por los intervinientes, imágenes o mensajes de telefonía móvil.
2. Los expedientes electrónicos podrán incluir un índice electrónico, firmado o sellado por el responsable encargado de su tramitación. Este índice garantizará la integridad del expediente electrónico y permitirá su pronta 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 en soporte papel.

■ ■ **Artículo 25. Terminación de los procedimientos por medios electrónicos**

1. De conformidad con lo previsto en el artículo 45.3 de la Ley 30/1992, los procedimientos que se tramiten y se acaben en soporte electrónico garantizarán la identificación y el ejercicio de la competencia por parte del órgano que, en cada caso, esté reconocido como competente.
2. El acto o resolución que ponga fin a un procedimiento electrónico deberá cumplir los requisitos previstos en el artículo 89 de la Ley 30/1992, e ir acompañado de la firma electrónica reconocida del órgano administrativo o personal municipal competente para dictar el acto o resolución.
3. El traslado de documentos electrónicos, incluidos los que deben figurar en los libros de resoluciones y en los libros de actas, mientras éstos no estén en soporte electrónico, se hará de acuerdo con el procedimiento de compulsas previsto en esta Ordenanza.

■ ■ **Artículo 26. La notificación telemática de los actos administrativos**

1. La notificación electrónica se podrá practicar utilizando medios electrónicos cuando el interesado haya elegido estos medios como preferentes o exprese su consentimiento a su utilización, en los procedimientos administrativos y trámites incorporados a la tramitación por vía electrónica.
2. La aceptación de los interesados podrá tener carácter general para todos los trámites que los relacionen con la Administración Municipal o para uno o varios trámites, según se haya manifestado. En los procedimientos administrativos electrónicos iniciados a instancia de parte, se presumirá la existencia de dicha aceptación, salvo que el mismo interesado haya manifestado lo contrario a través de los medios telemáticos que el Ayuntamiento le facilite.

3. Para la eficacia de lo dispuesto en el presente artículo, todo aquel interesado que manifieste su voluntad de recibir notificación por medios electrónicos deberá disponer de una dirección de correo electrónico habilitada para aquella finalidad, que será única para cada interesado.
 - a. La dirección o correo electrónico habrá de cumplir con los siguientes requisitos, bajo la exclusiva responsabilidad del interesado:
 - b. Poseer identificadores de usuario y clave o claves de acceso para garantizar la exclusividad de su uso.
 - c. Contar con mecanismos de autenticación que garanticen la identidad del usuario.
 - d. Disponer de mecanismos de cifraje para proteger la confidencialidad de los datos.
 - e. Cualquier otro que se fije normativamente.
4. La dirección de correo electrónico tendrá vigencia indefinida como dirección válida a efectos de notificación, excepto en los supuestos en que el titular solicite su revocación o modificación, por defunción de la persona física o extinción de la personalidad jurídica, cuando una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de las notificaciones, supuesto en el cual será comunicado al interesado para que pueda expresar su interés por mantenerla activa; en caso contrario, se inhabilitará la dirección de correo electrónico.
5. La notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el acceso a su contenido en la dirección de correo electrónico. El sistema de notificación deberá acreditar las fechas y horas en que se produzca la recepción de la notificación en la dirección electrónica del interesado y el acceso al contenido del mensaje de notificación por parte del ciudadano notificado, así como cualquier causa técnica que imposibilite alguna de las circunstancias anteriores.
6. Cuando haya constancia de la recepción de la notificación en la dirección electrónica y transcurran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada a los efectos previstos en el artículo 59 de la Ley 30/1992, salvo que de oficio o a instancia del interesado se compruebe la imposibilidad técnica o material del acceso a su dirección electrónica.
7. Durante la tramitación de los procedimientos, el interesado podrá requerir al órgano o entidad correspondientes que las notificaciones sucesivas no se practiquen por medios electrónicos, en cuyo caso se deberá usar cualquier otro medio admitido por el artículo 59 de la Ley 30/1992. Igualmente, durante la tramitación de un procedimiento no electrónico, el interesado podrá requerir al órgano o entidad correspondientes que las notificaciones sucesivas se practiquen en la forma prevista en esta Ordenanza.

■ ■ Artículo 27. Documentos y certificados administrativos electrónicos

1. La Administración Municipal establecerá los mecanismos necesarios para la emisión de documentos y certificados administrativos electrónicos, que producirán idénticos efectos que los expedidos en soporte papel, siempre que incorporen una o varias firmas electrónicas tal y como se establece en la Ley 59/2003. El contenido de éstos se podrá imprimir en soporte papel y la firma manuscrita será sustituida por un código de verificación generado electrónicamente, que permitirá comprobar su autenticidad accediendo telemáticamente a los archivos del órgano u organismo emisor.

2. La Administración Municipal emitirá certificados electrónicos sobre los datos que figuran en su poder, a petición de los ciudadanos.
3. Los ciudadanos, en sustitución de los certificados en papel, podrán presentar a la Administración Municipal certificados en soporte electrónico de otras Administraciones obtenidos telemáticamente o bien mediante la compulsión electrónica del certificado en papel.

■ **Capítulo 7º. Registro, archivo y acceso a los documentos electrónicos**

■ ■ **Artículo 28. Registro Electrónico de entrada y salida de documentos**

De conformidad con los artículos 24.1 y 25 de la Ley 11/2007 y el artículo 49 de la Ley 7/85, de 2 de Abril, Reguladora de las Bases de Régimen Local, y con la vigente legislación en materia de Régimen Local, mediante esta Ordenanza se crea y regula el funcionamiento del Registro Electrónico del Ayuntamiento de Rivas Vaciamadrid, de acuerdo con las siguientes normas:

1. El Registro Electrónico tiene carácter voluntario para los administrados, a excepción de los supuestos de utilización obligatoria establecidos por Ley y/o normas de creación de futuros procedimientos telemáticos donde se regule la presentación de solicitudes, escritos o comunicaciones a través del referido Registro Electrónico.
2. El Ayuntamiento de Rivas Vaciamadrid ha automatizado las oficinas de registro físicas a las que se refiere el artículo 38 de la Ley 30/1992, 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.
 - a. Aquellos documentos relativos a los procedimientos y asuntos que sean competencia de la Administración Municipal presentados en las oficinas de registro físicas del Ayuntamiento que superen las dimensiones del formato de papel estándar DIN A4 deberán ser presentados en formato digital (CD-ROM, memoria USB, disco duro portátil, tarjeta de memoria, etc.)
 - b. Todos los procedimientos y asuntos que sean competencia de la Administración Municipal que exijan la presentación de documentación, solicitudes, escritos o comunicaciones a través del Registro de entrada del Ayuntamiento tendrán la obligatoriedad de presentarse por medios electrónicos, en los supuestos previstos en el artículo 27.6 de la Ley 11/2007. Esta obligación puede extenderse, en su caso, a la práctica de notificaciones administrativas por medios electrónicos. 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 a través de los medios legales oportunos y en la sede electrónica del Ayuntamiento.
 - c. El Ayuntamiento dispone de regulación relativa a especificaciones técnicas de presentación documental en soporte electrónico en su “Ordenanza de Tramitación de Licencias Urbanísticas, Obras en Vía Pública y Actividades”, publicada en el B.O.C.M. número 170, de 18 de julio de 2008, y que en su “Art. 6. Soporte Documental”, indica:

“La presentación de solicitudes, escritos, planos, comunicaciones y documentos deberá efectuarse en papel, debidamente registrado, y/o en soporte informático, electrónico o telemático, siguiendo las instrucciones que el Ayuntamiento proporcione para facilitar la utilización de nuevas tecnologías.

El soporte informático será compatible con el software municipal, de conformidad con lo previsto en el anexo VIII de esta Ordenanza. En todo caso, los proyectos que se presenten en soporte informático deberán contar con el visado digital del colegio profesional correspondiente”.

El anexo VIII de dicha Ordenanza debido a su interés en referencia a la administración electrónica del Ayuntamiento se reproduce íntegramente en el Anexo III de la presente Ordenanza.

3. En el Registro Electrónico se podrán presentar solicitudes, escritos o comunicaciones relativos a los procedimientos y asuntos que sean competencia de la Administración Municipal y respecto de los cuales se haya establecido la posibilidad de su tramitación electrónica.

Cualquier solicitud, escrito o comunicación que los interesados presenten a través del Registro Electrónico y que no esté relacionado con los procedimientos y asuntos mencionados, no producirá ningún efecto y se tendrá por no presentado, comunicándose al interesado esta circunstancia e indicándole los registros y, en su caso, los lugares habilitados para su presentación de acuerdo con el artículo 38.4 de la Ley 30/1992.

4. El Registro Electrónico estará habilitado para la recepción y salida de documentos electrónicos. La fecha de entrada y/o de salida se acreditará mediante un servicio de consignación electrónica de fecha y hora.
5. El acceso al Registro Electrónico se realizará exclusivamente a través de la sede electrónica, de la cual se dará la oportuna publicidad para su conocimiento general. En cualquier caso, la dirección cumplirá además las exigencias de accesibilidad a personas con discapacidad.
6. En ningún caso tendrán la condición de Registro Electrónico los buzones de correo electrónico corporativo asignado a los empleados públicos o a las distintas concejalías y órganos municipales. Tampoco tendrán la consideración de Registro Electrónico los dispositivos de recepción de fax, salvo aquellos supuestos expresamente previstos en el ordenamiento jurídico.
7. Sin perjuicio de los efectos sustantivos que el Ordenamiento Jurídico atribuye a la presentación de solicitudes, escritos o comunicaciones, el Registro Electrónico estará a disposición de sus usuarios las veinticuatro horas al día, todos los días del año, excepto las interrupciones que sean necesarias por razones técnicas. El Registro Electrónico se regirá por la fecha y la hora oficiales en la circunscripción territorial de la Corporación.
8. La presentación de solicitudes, escritos y/o comunicaciones en el Registro Electrónico tendrán los mismos efectos que la presentación efectuada por el resto de medios admitidos por el artículo 38.4 de la Ley 30/1992.
9. El cómputo de plazos en las solicitudes, escritos y comunicaciones por el Registro Electrónico de la Corporación es el siguiente:
 - a. La fecha y hora de referencia serán los vigentes en el momento de la recepción o salida de la correspondiente solicitud, escrito o comunicación, en o desde el sistema de información que dé soporte al Registro Electrónico.
 - b. La entrada de solicitudes, escritos y/o comunicaciones recibidas en días inhábiles se entenderán efectuadas en la primera hora del primer día hábil siguiente. A estos efectos, constará en el asiento de entrada correspondiente la fecha y hora en que efectivamente se ha recibido la solicitud, escrito o comunicación presentada pero se indicará en el mensaje de confinación las cero horas y un minuto del siguiente día hábil.
 - c. No se dará salida, a través del Registro Electrónico, a ningún escrito o comunicación en día inhábil.
 - d. Se consideran días inhábiles, a efectos del Registro Electrónico de la Administración Municipal, los establecidos como días festivos en el calendario oficial de fiestas laborales de la Comunidad Autónoma de Madrid y de fiestas locales de este municipio.

10. En cualquier supuesto la presentación telemática de los documentos a que se refiere esta Ordenanza no implica la ampliación de los plazos establecidos por el Ordenamiento Jurídico.
11. Los datos contenidos en las solicitudes y, si procede, en el certificado, quedan anotadas automáticamente en el Registro Electrónico y constituyen los asientos registrales Electrónicos.
12. En aquellos casos en que se detecten anomalías de tipo técnico en la recepción telemática del documento, esta circunstancia deberá ser puesta en conocimiento del presentador por parte del propio sistema, mediante el correspondiente mensaje de error, a fin de que le conste que no se ha producido válidamente la presentación.
13. En el caso de la presentación de documentos electrónicos de cualquier tipo que contengan virus informáticos, programas espías o en general cualquier tipo de código malicioso, se considerará sin más trámite que no se ha producido la recepción del escrito, solicitud o comunicación, informando de ello al usuario mediante un mensaje al efecto.
14. El Registro Electrónico emitirá automáticamente un justificante de la recepción de los documentos electrónicos presentados, dirigido a la dirección electrónica de procedencia, autenticada mediante firma electrónica de la Administración, en el que constará el contenido íntegro del documento o documentos presentados y los datos de registro que se le asignen, datos que, como mínimo, serán los siguientes: número de anotación, día y hora de ésta.
15. El Registro Electrónico practicará un asiento de salida por cada documento electrónico que sea remitido en el que se hará constar: el número de referencia o registro, la fecha y la hora de emisión, el órgano de procedencia, la persona a la que se dirige, extracto o reseña del contenido y, en su caso, número de referencia del asiento de entrada.
16. Cuando por razones técnicas se prevea que el registro no podrá estar operativo, se deberá informar de ello a los usuarios con la máxima antelación posible y mientras dure esta situación.
17. Todos los documentos electrónicos que se presenten ante el Registro Electrónico deberán emplear formatos que sean compatibles con los utilizados por el Ayuntamiento.

■ ■ Artículo 29. Gestión de los documentos electrónicos

1. Originales en soporte informático:
 - Los documentos en soporte informático producidos válidamente por la Corporación y los demás órganos y entes actuantes tendrán la consideración de documentos originales, y se encontrarán debidamente grabados en los programas y aplicaciones de procedimiento por vías telemáticas, mientras se encuentren en fase activa.
 - Los documentos originales en soporte informático que se entreguen a las Administraciones actuantes deben poder ser impresos y archivados informáticamente, incluyendo la firma electrónica correspondiente.
2. Copias electrónicas:
 - El Secretario/a General de la Corporación o funcionario/a en quien delegue podrá emitir copias electrónicas con la consideración de copias auténticas de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, siempre que cumpla los siguientes requisitos:

- a. Asegurar la exactitud del contenido, aunque la estructura del documento se adapte a formatos o sistemas diferentes.
- b. Incluir una manifestación relativa a la comprobación de los elementos de autenticidad e integridad del documento original.
- c. Garantizar su autenticidad e integridad mediante la firma electrónica reconocida.

3. Compulsa electrónica de documentos en soporte papel:

Con las mismas condiciones señaladas en el número anterior, el Secretario/a General de la Corporación o funcionario/a en quien delegue podrá emitir copias electrónicas auténticas de documentos emitidos originalmente por los interesados o por las Administraciones Públicas en soporte papel.

La compulsa electrónica es el procedimiento de digitalización de la documentación en soporte papel y su comprobación por el Secretario/a General de la Corporación o funcionario/a en quien hubiere delegado, produciéndose una copia auténtica electrónica.

La compulsa electrónica se realizará a través de un procedimiento de digitalización seguro, que incluya la firma electrónica reconocida del personal al servicio de la Administración Municipal que haya realizado la compulsa y que garantice la autenticidad y la integridad de la copia, así como la identificación del órgano que realiza la compulsa, mediante la firma electrónica correspondiente.

Los documentos compulsados electrónicamente podrán ser válidos tanto en el procedimiento concreto para el que se ha realizado la compulsa como para cualquier otro procedimiento tramitado por la Administración Municipal.

4. Las copias auténticas electrónicas de documentos administrativos y los documentos compulsados electrónicamente tendrán la consideración de copias auténticas, a los efectos de lo previsto en el artículo 46 de la Ley 30/1992.

En consecuencia, las copias auténticas electrónicas disfrutará de la misma validez y efectos que los documentos originales. Las copias auténticas electrónicas indicarán la circunstancia de ser copias auténticas de documentos originales y, si corresponde, su fecha de caducidad. Las copias auténticas electrónicas deben poder ser impresas y archivadas informáticamente, incluyendo en todo caso la firma electrónica correspondiente.

5. Los documentos electrónicos se podrán trasladar a copias en soporte papel mediante procedimientos automatizados. En este caso, el documento en soporte papel incorporará un mecanismo que permitirá validar su contenido con la identificación del documento electrónico original. El acceso al documento electrónico original se podrá realizar a través de una dirección electrónica facilitada por la Administración Municipal.

■ ■ Artículo 30. El archivo electrónico del Ayuntamiento de Rivas Vaciamadrid

1. El Archivo Electrónico tiene como misión la conservación, organización y servicio de los documentos producidos y recibidos por el Ayuntamiento en el ejercicio de sus funciones, según indica el Artículo 24.1 de la Ley 4/1993, de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid.
2. La Administración Municipal podrá archivar por medios electrónicos todos los documentos que se produzcan en el ejercicio de sus funciones, de manera que se cumplan los términos previstos en el artículo 45.5 de la Ley 30/1992.

3. La Concejalía responsable de la Administración Electrónica del Ayuntamiento, determinará las políticas de creación y conservación del archivo digital, así como los criterios de control sobre la documentación del archivo electrónico: migración de los datos, ingreso de datos, conservación de datos, normas, acceso de seguridad y validación. Así mismo, determinarán las políticas de renovación de los soportes, actualización de los programas y de estrategias para garantizar la capacidad de lectura de los documentos con el transcurso del tiempo.
4. El Archivo Electrónico del Ayuntamiento tendrá como funciones principales: la descripción documental (metadatos), la gestión de fondos (transferencias, migraciones, selección y evolución), la gestión de usuarios, las auditorías de uso y circulación de documentos, la gestión de accesos (protección y seguridad de datos) y el control de autenticidad e integridad documental (validez jurídica).

■ ■ Artículo 31. Normas sobre el archivo de los documentos

El archivo de los documentos en soporte informático y las medidas de conservación de los documentos en apoyo informático de los procedimientos se ajustará a los siguientes principios de actuación, tratamiento y validez:

a. Archivo de documentos en soporte informático:

Los documentos en soporte informático, resultantes de la aportación a la Administración Municipal de información, solicitudes, certificados electrónicos y documentos por parte del interesado, o que hayan sido obtenidos mediante comunicaciones de datos administrativos de terceras administraciones, deben ser gestionados y archivados exclusivamente en soporte informático, de acuerdo con las prescripciones de la normativa legal de aplicación a este tipo de documentos.

b. Medidas de conservación de documentos en soporte informático:

Los servicios y los programas y aplicaciones de procedimiento por vías telemáticas han de establecer las medidas necesarias para garantizar la conservación, integridad, autenticidad, calidad, protección y, cuando sea necesario, la confidencialidad de los documentos en soporte informático, aplicándose entre otras las medidas siguientes:

- La actualización criptográfica del documento firmado: mediante la adición de un nuevo sello de fecha y hora.
- El registro del documento firmado electrónicamente: en un soporte físico perdurable, con garantía de la fecha de entrada.
- La implantación de un sistema de identificación de los usuarios y de control de accesos y, en general, el cumplimiento de todas las garantías previstas en la legislación de protección de datos.

c. Los documentos originales en soporte informático podrán transformarse, para adaptar su formato a las necesidades de gestión y preservación previstas, de acuerdo con las siguientes normas:

- El cambio de formato deberá garantizar la exactitud del contenido del documento anterior, así como la comprobación de los elementos de autenticidad e integridad del documento original. El documento resultante de la transformación será firmado electrónicamente por el órgano competente o empleado municipal para la transformación.
- El paso del documento en soporte informático a papel se realizará excepcionalmente, y deberá permitir la verificación técnica de la firma del órgano competente o empleado municipal.

■ ■ Artículo 32. Responsabilidad

El Ayuntamiento no responderá del uso fraudulento que los usuarios del sistema puedan llevar a cabo de los servicios prestados mediante E-administración. Dichos usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su autenticación en el acceso a estos servicios de 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. Será responsabilidad del usuario la adecuada custodia y manejo de los ficheros que le sean devueltos por el Registro Electrónico como recibo de presentación.

■ Capítulo 8º. Servicio telemático de pagos

■ ■ Artículo 33. Servicio Telemático de Pagos

1. El pago de los tributos, precios públicos y demás ingresos de derecho público de los que sea acreedora la Administración Municipal podrá realizarse por vía telemática de acuerdo con el procedimiento que se regula en este capítulo.
2. El pago podrá ser realizado tanto por los propios obligados al pago, como por medio de terceros que actúen en su representación, conforme a lo previsto en los artículos 11 y 20 de esta Ordenanza.

Quien ordene un pago en nombre de un tercero sin contar con representación o mandato suficientes estará sujeto a las responsabilidades correspondientes cuando dicho pago hubiese ocasionado un perjuicio a la persona en cuyo nombre se hizo el pago o a un tercero.

3. Los pagos podrán realizarse por cualquier medio admitido por el Servicio Telemático de Pagos y por cualquier entidad financiera de entre las adheridas al mismo. En particular, podrán realizarse los pagos mediante cargo en cuenta bancaria desde una cuenta corriente abierta en una entidad financiera adherida o mediante una tarjeta de crédito o débito emitida por una entidad financiera adherida.
4. El pago telemático se instrumentará a través de la plataforma creada por la entidad pública Red.es, en el marco del Convenio de colaboración entre la asociación española de banca, la confederación española de cajas de ahorros, la unión nacional de cooperativas de crédito y la entidad pública empresarial red.es para la prestación del servicio de pago telemático en la Administración Pública.

La Junta de Gobierno Local podrá acordar la adhesión a cualquier otra plataforma de pagos de análogas características, aceptando y aprobando las normas técnicas que resulten necesarias.

5. La adhesión de las entidades financieras interesadas a la plataforma de pagos telemáticos utilizada por la Administración Municipal se realizará conforme al procedimiento y requisitos técnicos previstos para la citada plataforma. Así mismo, el Ayuntamiento podrá validar sistemas alternativos de pagos telemáticos garantizando en todo momento la seguridad del procedimiento.
6. La realización del pago por medio telemático no supone alteración alguna en cuanto a las obligaciones formales de cualquier clase de las que sea responsable el interesado en relación con el concepto por el que se haya realizado el pago, en particular las relativas a la conservación de la documentación y a la presentación de la documentación exigida en el registro municipal.

7. La imposibilidad, por el motivo que fuere, de realizar la transacción por el sistema de pago telemático, no excusarán al obligado al pago de realizar dicho pago dentro de los plazos establecidos en la normativa de los correspondientes tributos, precios públicos y demás ingresos de derecho público.

■ ■ Artículo 34. Procedimiento del Servicio Telemático de Pago

1. El importe a pagar, en función de las características propias del concepto a abonar, podrá venir fijado por la corporación o ser determinado por los interesados mediante los formularios y/o aplicaciones disponibles en la página web del Ayuntamiento.
2. Una vez determinado el importe a pagar, el usuario utilizará un certificado de firma electrónica reconocida para dar la orden de pago necesaria para tramitar el pago por el medio de pago elegido. La Administración Municipal y/o la entidad pública Red.es custodiarán durante cinco años la información relativa al no repudio de la orden de pago.
3. La información relativa al pago, una vez validada la firma digital, se enviará a la entidad financiera adherida al sistema de pago telemático elegida por el ordenante, conforme al procedimiento previsto en la plataforma de pago telemático.
4. La entidad financiera adherida, previa la realización de las comprobaciones que procedan según el medio de pago:
 - a. Devolverá un mensaje de error, si fuese rechazado el cargo.
 - b. Efectuará el cargo en el medio de pago elegido por el ordenante del pago y realizará el abono en la cuenta restringida de recaudación de tributos de la Administración Municipal generándose un Número de Referencia Completo (NRC) mediante un sistema criptográfico que permitirá asociar la orden de pago al pago de ella derivado.
5. La generación del NRC por la Entidad Financiera Colaboradora implicará:
 - a. Que la Entidad Financiera Colaboradora deberá realizar el abono en la cuenta restringida de recaudación.
 - b. Que el recibo en el que figura responde a un ingreso realizado en la Entidad Financiera Colaboradora que lo expide.
 - c. Que dicho recibo corresponde a la liquidación incorporada en el justificante de pago y no a otra.
 - d. Que a partir del momento de generación del NRC queda la Entidad Financiera obligada frente a la Administración Municipal por el importe que figura en dicho justificante de pago, quedando el obligado al pago liberado de su obligación frente a la Administración Municipal.
 - e. Una vez generado el NRC no se admitirá la retrocesión del pago por parte de la Entidad Financiera, debiendo presentar el ordenante del pago, en su caso, ante la Administración Municipal, la correspondiente solicitud de devolución de ingresos indebidos.
6. La Entidad Financiera que haya generado el correspondiente NRC conservará durante cinco años los soportes informáticos que lo motivaron.

7. La Entidad Financiera adherida comunicará a la Administración Municipal la confirmación del cobro efectuado. Única y exclusivamente a la recepción del NRC, la Administración Municipal presentará al ordenante del pago un justificante de pago electrónico, una vez que valide la coherencia de la transacción con el NRC. El justificante de pago emitido conforme a lo establecido en este artículo, podrá imprimirse y surtirá los efectos liberatorios para con la Administración Municipal señalados en el Reglamento General de Recaudación.

■ *Disposiciones transitorias*

■ ■ PRIMERA. Incorporación de trámites y procedimientos actuales

Los trámites y procedimientos disponibles actualmente para la tramitación por vía electrónica de procedimientos que se relacionan en el anexo I de esta Ordenanza, se considerarán incorporados a la tramitación por vía electrónica y se deberán incluir en el catálogo de trámites y procedimientos electrónicos del Municipio desde el momento de entrada en vigor de esta Ordenanza.

■ ■ SEGUNDA. Procedimientos y Ordenanzas en curso

Esta Ordenanza no se aplicará a los procedimientos iniciados con anterioridad a su entrada en vigor.

Las Ordenanzas en vigor del Ayuntamiento quedarán obligadas, en el momento de aprobación de la presente Ordenanza, a exigir, en todos los procedimientos y asuntos que sean competencia de la Administración Municipal, la presentación de toda la documentación, solicitudes, escritos o comunicaciones a través del Registro de entrada del Ayuntamiento por medios electrónicos, en los supuestos previstos en el artículo 27.6 de la Ley 11/2007. Dicha modificación de las Ordenanzas existentes deberá ser publicada en la sede electrónica.

■ ■ TERCERA. Derecho a no presentar datos y documentos existentes

El derecho de los ciudadanos a no presentar datos y documentos en poder de la Administración Municipal, recogido en el artículo 8.c., se dará cumplimiento en la medida que las herramientas tecnológicas lo permitan, ampliándose ese derecho al resto de Administraciones Públicas en el momento en el que la tecnología, la interoperabilidad para la transmisión de datos entre Administraciones Públicas y demás factores implicados lo haga posible. Deberán en todo momento regirse por el artículo 9 de la Ley 11/2007.

■ ■ CUARTA. Reunión virtual de órganos colegiados

Si los medios técnicos disponibles lo permiten, los órganos colegiados de la Administración Municipal no propiamente regulados en la normativa local, podrán constituirse y adoptar acuerdos utilizando medios electrónicos, con respeto a los trámites esenciales establecidos en los artículos 26 y 27 de la Ley 30/1992, 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 avalará la participación de los miembros conforme 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.

■ ■ **QUINTA. Tablón de edictos electrónico**

El tablón de edictos electrónico entrará en funcionamiento en un plazo máximo de un año desde la entrada en vigor de esta Ordenanza.

■ ■ **SEXTA. Notificación electrónica**

El Ayuntamiento pondrá en marcha la notificación electrónica, para los procedimientos y trámites que lo requieran, en un plazo máximo de seis meses desde la entrada en vigor de esta Ordenanza.

■ ■ **SÉPTIMA. Registro Electrónico**

El Registro Electrónico regulado en esta Ordenanza entrará en funcionamiento a las cero horas del día siguiente de su entrada en vigor.

La Concejalía competente en materia de modernización administrativa elaborará un Reglamento interno de funcionamiento del Registro Electrónico, que se deberá emitir y publicar en el plazo máximo de un año desde la entrada en vigor de esta Ordenanza.

■ ■ **OCTAVA. Archivo electrónico**

La Concejalía competente en materia de modernización administrativa elaborará una propuesta técnica de organización, funcionamiento y puesta en marcha del archivo municipal electrónico, que se deberá emitir en el plazo máximo de un año desde la entrada en vigor de esta Ordenanza.

■ ■ **NOVENA. Representación electrónica**

La representación electrónica, regulada en los artículos 11, 20 y 33.2 de la presente Ordenanza, entrará en funcionamiento en momentos diferentes según el trámite y el procedimiento a realizar, en la medida que lo permitan las disponibilidades presupuestarias de la Corporación, tal y como indica el punto 4 de la Disposición final tercera de la Ley 11/2007.

■ ■ **DÉCIMA. Listado de funcionarios**

El Ayuntamiento mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación de los ciudadanos por funcionario público.

■ *Disposiciones finales*

■ ■ PRIMERA. Difusión de la Ordenanza

Tan pronto como sea aprobada esta Ordenanza, el Ayuntamiento de Rivas Vaciamadrid la difundirá por los medios electrónicos de que disponga.

■ ■ SEGUNDA. Formación de los empleados públicos municipales

La Administración Municipal promoverá la formación del personal a su servicio en la utilización de medios electrónicos para el desarrollo de sus actividades.

■ ■ TERCERA. Teletrabajo en la Administración Municipal

La Administración Municipal adoptará las medidas necesarias para fomentar e implantar progresivamente el teletrabajo del personal a su servicio, regulando las condiciones en las que se realizará.

■ ■ CUARTA. Contratación administrativa

La Administración Municipal adoptará las medidas necesarias para fomentar e implantar progresivamente la contratación por vía electrónica y el uso de la factura electrónica por parte de sus contratistas.

■ ■ QUINTA. Reutilización de Información

La Administración Municipal regulará mediante Ordenanza Municipal las condiciones aplicables a la reutilización de los documentos elaborados o custodiados por el Ayuntamiento, de acuerdo a la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información en el Sector Público.

■ ■ SEXTA. Regulación de nuevos procedimientos y trámites

A partir de la entrada en vigor de esta Ordenanza, cualquier regulación que se efectúe de nuevos procedimientos y trámites administrativos, o modificación de los existentes, deberá prever la posibilidad de su tramitación por medios Electrónicos y se ajustará a los requisitos previstos en esta Ordenanza.

■ ■ SÉPTIMA. Adaptación a la normativa municipal

El Ayuntamiento se compromete a adaptar la normativa municipal a las previsiones de esta Ordenanza.

■ ■ OCTAVA. Entrada en vigor

Esta Ordenanza se publicará en el Boletín Oficial de la Comunidad de Madrid, entrando en vigor transcurridos quince días hábiles desde su publicación, de acuerdo con lo previsto en los artículos 70.2 y 65.2 de la Ley 7/1985, de 2 de abril, Reguladora del Régimen Local.

■ **Anexo I. Trámites y gestiones municipales disponibles actualmente a través del portal del Ayuntamiento de Rivas Vaciamadrid, www.rivas-vaciamadrid.org**

A partir del 1 de enero de 2010 y sin perjuicio de la progresiva implantación electrónica de los restantes trámites y procedimientos, el Ayuntamiento pone a disposición de los ciudadanos el acceso electrónico al siguiente listado de trámites y gestiones administrativas:

■ ■ **Solicitudes y trámites públicos (sin necesidad de identificación):**

- Incidencias en Carpeta Ciudadana
- Solicitud de Alta en Carpeta Ciudadana

Simulaciones de:

- Impuesto de Obra Mayor
- Impuesto de Obra Menor
- Impuesto de vehículos
- Tasa de Obra Mayor
- Tasa de Obra Menor
- Plusvalías

■ ■ **Solicitudes y trámites privados (necesaria identificación):**

- Cambio de cuenta de domiciliación
- Certificado de empadronamiento
- Certificado de empadronamiento colectivo
- Comunicación de cambio de domicilio fiscal
- Domiciliación bancaria
- Solicitud de bonificación del impuesto sobre vehículos del tracción mecánica (IVTM) para discapacitados
- Solicitud de bonificación del impuesto sobre vehículos del tracción mecánica (IVTM) para vehículos históricos
- Incidencias en Carpeta Ciudadana
- Solicitud de alta en la Red WiFi de los edificios municipales del Ayuntamiento de Rivas Vaciamadrid.
- Pago y gestión de recibos.
- Consulta de expedientes.
- Consulta de Registro de salida y entrada.
- Emisión automática de volantes de empadronamiento individual y colectivo.
- Consulta de Unidades Fiscales.

■ ■ Principio del formulario. Autoliquidaciones y simulaciones de (incluido la posibilidad de pago):

- Autoliquidación Impuesto de Obra Mayor
- Autoliquidación Impuesto de Obra Menor
- Autoliquidación Impuesto de vehículos
- Autoliquidación Tasa de Obra Mayor
- Autoliquidación Tasa de Obra Menor
- Plusvalías

■ **Anexo II. Características de las aplicaciones informáticas de registro y tramitación electrónica utilizadas por el Ayuntamiento de Rivas Vaciamadrid**

Las aplicaciones informáticas que dan soporte a las gestiones de tramitación electrónica y Registro Electrónico del Ayuntamiento de Rivas Vaciamadrid se basan en dos tipos de sistemas:

- Aplicaciones Web que utilizan comunicación mediante un servidor Web seguro con protocolo de seguridad SSL y en las cuales la seguridad de acceso de los usuarios está basada en certificados digitales X.509.
- Aplicaciones de gestión interna del Ayuntamiento de Rivas Vaciamadrid, basadas en arquitectura cliente-servidor, las cuales se migrarán a una arquitectura en tres capas desarrollada en estándares abiertos según el plan de migración de la Concejalía de Modernización Administrativa y Atención a la Ciudadanía.

Los usuarios que quieran utilizar las aplicaciones informáticas de Registro Electrónico y tramitación electrónica del Ayuntamiento de Rivas Vaciamadrid deberán contar con equipos que reúnan las características y configuración que en cada caso se establezcan, estando estos requerimientos técnicos definidos en la Web municipal o en su defecto en la página de inicio de cada aplicación.

■ **Anexo III. Normas para el suministro de cartografía de proyectos y obras y de digitalización**

■ ■ I. Cartografía de proyectos y obras

Esta normativa será de aplicación a todas aquellas actuaciones urbanísticas que precisen de un proyecto para su ejecución, el cual incida sobre la definición geométrica del trazado de elementos significativos, o que afecten a la configuración u ordenación del territorio del Municipio.

El Ayuntamiento de Rivas-Vaciamadrid a mediados de 2006 inició una cartografía a partir de un vuelo de todo su Término Municipal.

La base para el desarrollo de los trabajos fueron las ortofotos obtenidas. La actualización y conservación de la cartografía se realizará a partir de la Red Topográfica, conjunto de señales fijas distribuidas por todo el suelo urbano. Esta red tiene como fin el que los topógrafos, mediante el posicionamiento sobre ellas de aparatos específicos, efectúen las observaciones y medidas necesarias para desarrollar los trabajos de determinación de superficies de parcelas, replanteo de calles, urbanización y análogos.

La documentación a presentar al Ayuntamiento ha de reunir una serie de requisitos que se especifican a continuación, con el fin de aunar toda la información en una cartografía unificada. De modo que el Ayuntamiento pueda integrar la misma en las Bases de Datos para su correcta explotación.

■ ■ II. Normativa de digitalización

Los elementos a digitalizar deben cumplir una serie de criterios obligatorios. El objetivo es la normalización de todos los proyectos a entregar en la Oficina de Información Territorial (OITR) permitiendo la integración final de los mismos en la cartografía del Ayuntamiento de Rivas-Vaciamadrid.

■ *Verificación*

La documentación cartográfica que acompaña al proyecto será revisada por el personal de la Oficina de Información Territorial (OITR), no dándose por válido a todos los efectos hasta que no sea emitido un informe favorable de la misma.

■ *Criterios de referenciación cartográfica*

Los archivos deben cumplir unos criterios cartográficos de georreferenciación afines a los archivos del propio Ayuntamiento.

- La digitalización se ha de realizar tomando como referencia los vértices geodésicos instalados en el municipio de Rivas Vaciamadrid.
- El Ayuntamiento facilitará al proyectista las reseñas y datos numéricos (X, Y, Z) a través de la Oficina de Información Territorial, de los puntos fijos de la Red Topográfica Municipal que se encuentren en la citada zona o a través de la página web del Ayuntamiento (www.rivas-vaciamadrid.org).
- Si para cubrir la zona a levantar, no fuese suficiente con las señales existentes de la Red, el Ayuntamiento, a través de la Oficina de Información Territorial, facilitará un fichero en formato DWG/DXF de la zona afectada previa solicitud por Registro.
- Los ficheros de dibujo correspondientes a los planos de emplazamiento o planta general del proyecto se presentarán en formato DWG/DXF, no pudiendo estar digitalizados en coordenadas 0,0, sino referirse a los puntos geodésicos municipales, de forma que se definan las coordenadas para el sistema de proyección UTM con sistema de coordenadas ED 50.
- Los datos digitalizados deben presentar coordenadas X, Y, Z referidas a la Red Topográfica Municipal en proyección UTM antes mencionada.

■ *Criterios generales*

- El soporte de entrega de los trabajos a realizar será en formato DWG/DXF.
- La escala será 1:1.

- Se deben generar las capas del proyecto utilizando los siguientes elementos básicos de digitalización: polilínea, línea, punto y polilínea cerrada (polígonos).
- No introducir líneas como b-spline y líneas suavizadas.
- Estas líneas, cuando generan un elemento cerrado, deben digitalizarse en un solo trazo. No ha de haber un conjunto de líneas sueltas.
- Asimismo, no deben darse casos en los que haya duplicación de líneas en la misma capa, cuando existan elementos contiguos, como por ejemplo dos parcelas adyacentes dentro de una manzana.
- Debe existir en los casos que lo precisen, las siguientes capas: manzana (polilínea cerrada), parcela (polilínea cerrada), subparcela (polilínea cerrada), parcela_urbanización (polilínea cerrada), edificio_pta_baja (polilínea cerrada), edificio_pta_tipo (polilínea cerrada), edificio_pta_alero_vuelos (polilínea cerrada), piscina (polilínea cerrada), txt_números_policía (texto simple), eje_calle (polilínea), division_propiedad (línea), txt_nombre_calle (texto simple), acera (polilínea cerrada), árbol (punto o bloque con pto. inserción centrado).

■ Prototipo de capas

CAPA	COLOR	TIPO LÍNEA
Manzana	241	Continuo
Parcela	21	Continuo
Subparcela	21	Continuo
Parcela	21	Continuo
Edificio Pta. Baja	1	Continuo
Edificio Pta.	1	Continuo
Edificio Pta. Alero Vuelos	1	Continuo
Piscina	150	Continuo
División Propiedad	8	Continuo
Eje_calle	7	Continuo
Acera	1	Continuo
Árbol	252	Continuo
Txt. Número Policía	7	Continuo
Txt. Nombre Calle	7	Continuo

- Cada capa contendrá un solo conjunto de elementos del mismo tipo (no mezclar líneas, puntos y polígonos).
- Todos estos elementos se digitalizarán en X, Y, Z.

- Los atributos de los elementos representados en cada capa deben ser comunes. No debe haber variaciones de propiedades entre elementos de una misma capa. (Nota: Propiedades “por capa”). El grosor de línea deberá ser “por defecto”.
- Rigurosidad geométrica y topológica: no deben aparecer elementos redundantes, inexistentes, mal codificados o digitalizados, de longitud cero, micropolígonos.

Se deben cerrar los elementos que se refieran a superficies, y existir conectividad entre elementos.

- Las referencias a objetos deben estar activadas y correctamente configuradas para obtener una correcta geometría y topología. De modo que una vez digitalizada la información, no existan elementos mal cerrados, sin conectividad o con excesivos segmentos en su trazado.
- Los elementos de texto pertenecientes a cada capa TXT_ deben de digitalizarse en una línea única de texto como grupo conjunto.

■ **Relieve. Modelo digital del terreno (MDT)**

Se representará la topografía del terreno mediante curvas de nivel, las cuales presentan entre sí una distancia de 0,5 metros. Las curvas directoras serán las de cota múltiplo de 2,5 metros.

■ **Digitalización de redes**

Para la digitalización de capas donde existan redes (agua, gas, telecomunicaciones, electricidad y análogos.) Se deben seguir las siguientes premisas:

- La red ha de ser digitalizada en segmentos conectados entre sí, de modo que las intersecciones siempre estén unidas por los puntos finales de cada línea o polilínea de dicha red. Cada tramo de red debe estar comprendido entre intersecciones y no podrán existir tramos que conecten con línea continua; esta deberá dividirse en tramos.
- Los textos identificativos deberán estar en una capa texto diferente.
- Si existiesen bloques dentro de la red (colectores, pozos y análogos), será el punto de inserción el que una los tramos.

Sede Electrónica: <https://www.rivas-vaciamadrid.org>

9.3. Ayuntamiento de Irún



■ Ordenanza municipal Reguladora de la Administración Electrónica

INDICE

EXPOSICIÓN DE MOTIVOS

TITULO PRELIMINAR (Arts. 1-4)

TITULO I. De los derechos de la ciudadanía en relación con la administración electrónica y del catálogo de servicios electrónicos

Capítulo 1º. De los derechos de la ciudadanía en relación a la administración electrónica (Arts. 5-8)

Capítulo 2º Del catálogo de trámites, servicios y procedimientos electrónicos. (Arts. 9-10)

TITULO II. Del régimen jurídico de la administración electrónica

Capítulo 1º. De la sede electrónica. (Arts. 11-13)

Capítulo 2º De la función de información y su difusión por medios electrónicos (Arts. 14-16)

Capítulo 3º De la identificación y autenticación (Arts. 17-23)

Capítulo 4º Del registro telemático (Arts. 24-26)

Capítulo 5º. De las comunicaciones electrónicas (Arts. 27-28)

TITULO III. De la gestión electrónica de los procedimientos

Capítulo 1º. De los principios de actuación en la gestión electrónica de los procedimientos (Arts. 29-30)

Capítulo 2º De la utilización de medios electrónicos en la tramitación de los procedimientos (Arts. 31-37)

Capítulo 3º De los documentos y los archivos electrónicos (Arts. 38-42)

TITULO IV. De la factura electrónica y el pago electrónico (arts. 43-44)

DISPOSICIONES ADICIONALES

DISPOSICIONES FINALES

■ Exposición de motivos

En los últimos tiempos el Ayuntamiento de Irún ha venido mostrando una constante preocupación por prestar a la ciudadanía un mejor servicio, aplicando políticas de calidad en la Administración como técnica para el logro de la excelencia en el servicio. En este sentido, desde instancias municipales ha existido siempre el convencimiento de que una adecuada atención al ciudadano, elemento básico de la Calidad de Servicio, se traduce en un progreso del propio servicio, al mejorar la comunicación con el usuario y colaborar con la eficiente resolución de los asuntos que éste demanda, reduciendo al mismo tiempo los costes en los que incurre la organización a la hora de prestar un servicio determinado y proyectando una imagen más positiva de la Administración hacia el conjunto de la ciudadanía.

La apertura del Servicio de Atención Ciudadana (S.A.C.) a comienzos de 1997 supuso, en ese aspecto, un salto cualitativo en la atención al ciudadano, puesto que llevaba aparejada consigo la evolución de una organización vertical hacia una estructura horizontal orientada directamente al ciudadano, a través de la instauración de un sistema de atención basado en la política de “*ventanilla única*”, que posibilitase la resolución de las principales demandas ciudadanas en un solo acto. Este hecho, junto con la puesta en práctica de políticas de normalización y modernización administrativa, ha posibilitado que el Ayuntamiento de Irun haya venido ofreciendo a la ciudadanía unos servicios de calidad a través del canal presencial y telefónico, que ahora pretenden extenderse al canal telemático.

Tras la reforma de la Ley 7/1985, de 2 de abril, de Bases del Régimen Local, acometida en el año 2003, el legislador introdujo un nuevo artículo 70 bis, cuyo apartado tercero contiene un mandato expreso dirigido a especialmente a los municipios para el impuso de la utilización interactiva de las tecnologías de la información y la comunicación, en aras a facilitar la participación y la comunicación con los vecinos, la presentación de documentos, y la realización de trámites administrativos, de encuestas y, en su caso, de consultas ciudadanas. Este precepto legal supuso la concreción, para las entidades locales, del mandato que ya se contenía 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, que ha sido, a su vez, recientemente desarrollado por la Ley 11/2007, de 22 de junio, de acceso electrónico de la ciudadanía a los Servicios Públicos. El contenido de esta última ley conlleva un completo reconocimiento del derecho que asiste a la ciudadanía para relacionarse con la Administración por medios electrónicos, lo cual supone, a su vez la necesidad de habilitar, por parte del Ayuntamiento de Irun, dicho canal de comunicación y relación con la ciudadanía, impulsando a través de este canal las mismas políticas de calidad de servicio que hasta la fecha han venido guiando la actividad municipal prestada a través de los otros dos canales de atención.

Teniendo en cuenta todo lo anterior, el Ayuntamiento de Irun, consciente de esta obligación legal y convencido de la oportunidad que ello implica para acercar la Administración y ofrecer un mejor servicio a la ciudadanía, aprueba la presente Ordenanza al objeto de establecer los compromisos y obligaciones que aquél asume en relación a la puesta en marcha del canal telemático, como tercera vía para el disfrute de los servicios municipales por parte de la ciudadanía. Esta Ordenanza establece, por lo tanto, el marco normativo en el que el Ayuntamiento de Irun asume el compromiso de impulsar una administración que emplee los medios electrónicos disponibles para facilitar la relación de la ciudadanía con su Administración más cercana, mejorando con ello el servicio ofrecido a los ciudadanos y posibilitando que la Administración municipal sea accesible para éstos las 24 horas del día y los siete días de la semana. A su vez, esta Ordenanza complementa lo ya dispuesto en la Ordenanza reguladora del S.A.C., aprobada por acuerdo plenario de 30 de octubre de 1996, adaptando sus disposiciones al procedimiento de tramitación telemático.

La Ordenanza se estructura en cinco Títulos (incluyendo el Título Preliminar), dos Disposiciones Adicionales y dos Disposiciones Finales. En el Título Preliminar se establece el objeto y ámbito de aplicación de la Ordenanza, así como una serie de definiciones y principios generales que guían la actuación del Ayuntamiento en materia de administración electrónica.

En el Título Primero se definen los derechos de la ciudadanía en materia de administración electrónica, los sistemas de acceso a los servicios electrónicos, así como aquellos mecanismos para la definición del catálogo de trámites, servicios y procedimientos electrónicos.

El Título Segundo se ocupa de los aspectos básicos del régimen jurídico de la administración electrónica, regulando las sedes electrónicas, el acceso a la información, las formas de identificación y autenticación, la representación para la realización de trámites electrónicos, el registro telemático y las comunicaciones electrónicas.

El Título Tercero regula la gestión electrónica de los procedimientos y expedientes administrativos, fijando los criterios que fundamentan dicha tramitación, sus diferentes fases, y la propia terminación del procedimiento. Se establecen, igualmente, los requisitos para la práctica de la notificación por medios electrónicos, así como las características y régimen jurídico aplicable a los documentos y archivos electrónicos, además de a la compulsa electrónica de documentos.

Por último, el Título Cuarto habilita la posibilidad de presentación de facturas al cobro en formato electrónico, y la posibilidad de abono de las mismas mediante la utilización de esos mismos medios.

La presente Ordenanza prescribe, ya en sus disposiciones adicionales, la creación de una Comisión Técnica de Administración Electrónica en el seno del Ayuntamiento de Irun, con el fin de promover, planificar y coordinar la implantación efectiva de los medios electrónicos en el funcionamiento de la Administración municipal.

■ *Título preliminar*

■ ■ **Artículo 1. Objeto**

1. La presente Ordenanza regula la implantación progresiva de la Administración Electrónica en el Ayuntamiento de Irun, facilitando la prestación de servicios a la ciudadanía a través de medios electrónicos, y garantizando que la interacción con todo tercero, en el ámbito de la actividad administrativa, se pueda materializar a través de la utilización de las tecnologías de la información.
2. El Ayuntamiento de Irun garantizará el derecho de los ciudadanos a relacionarse con el mismo utilizando medios electrónicos para el ejercicio de sus derechos, en los términos previstos en la Ley 11/2007, de 22 de junio, de acceso electrónico de la ciudadanía a los Servicios Públicos, o normativa que la sustituya. A este respecto, el Ayuntamiento de Irun asegurará la información, la accesibilidad, la integridad, la autenticidad, la seguridad, la confidencialidad y la conservación de los datos, documentos, informaciones y servicios que se gestionen en el ejercicio de sus competencias, promoviendo en todo momento la calidad de los servicios públicos prestados a través de medios electrónicos.

■ ■ **Artículo 2. Ámbito de aplicación**

1. La presente Ordenanza será de aplicación a los organismos públicos y entidades que conforman la Administración Municipal, englobando a:
 - a. Las Áreas y Servicios que integran el Ayuntamiento de Irun
 - b. Los Organismos Autónomos dependientes del Ayuntamiento de Irun
 - c. Las Entidades Públicas Empresariales que se pudiesen crear por parte del Ayuntamiento de Irun, vinculadas al mismo.
 - d. A las personas físicas, jurídicas y entes sin personalidad en sus relaciones con las Entidades incluidas en el ámbito de aplicación.
2. Las Sociedades Públicas y demás Entes Públicos de derecho privado, en las que la participación directa o indirecta del Ayuntamiento de Irun resulte mayoritaria, adoptarán las medidas oportunas para posibilitar, en el marco de la prestación de servicios públicos de competencia municipal, la prestación de los mismos a través de medios electrónicos, con sujeción a los principios expuestos en la presente Ordenanza cuando desarrollen actividades sujetas al derecho público.

3. Lo dispuesto en el apartado anterior será de aplicación, igualmente, a las empresas concesionarias de servicios públicos de competencia municipal, en el ámbito de prestación de dichos servicios públicos. A estos efectos, la Administración Municipal podrá reflejar en sus pliegos de contratación la obligación del adjudicatario de prestación de los servicios a través de medios electrónicos.
4. La presente Ordenanza no será de aplicación a la Administración Municipal y los organismos públicos dependientes de la misma en las actividades que desarrollen en régimen de derecho privado, limitándose su aplicación al ejercicio de potestades públicas en el ámbito competencial de aquéllos.

■ ■ Artículo 3. Definiciones

A los efectos de la presente Ordenanza, se entenderá por:

- **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.
- **Aplicación:** Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.
- **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.
- **Canales:** Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el telemático, así como otros que existen en la actualidad o pudieran existir en el futuro (dispositivos móviles, TDT...)
- **Certificado electrónico:** Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica: *“documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad”.*
- **Certificado electrónico reconocido:** Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica: *“son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten”.*
- **Ciudadanía:** Conjunto de personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones Públicas.
- **Dirección Electrónica:** Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.
- **Documento electrónico.** Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado, y susceptible de identificación y tratamiento diferenciado.

- **Estándar abierto:** Aquél que reúna las siguientes condiciones:
 - Sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso.
 - Su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.
- **Firma electrónica:** Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, *“conjunto de datos de forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”*.
- **Firma electrónica avanzada:** Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, *“firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control”*.
- **Firma electrónica reconocida:** Según el 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”*.
- **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.
- **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.
- **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.
- **Sistema de firma electrónica:** Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.
- **Sellado de tiempo:** Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.
- **Actividad de servicio:** Cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración.
- **Prestador de actividad de servicio:** Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

■ ■ Artículo 4. Principios generales en materia de Administración Electrónica

La actuación de la Administración Municipal de Irun en materia de Administración Electrónica se regirá por los siguientes principios:

- **Principio de Servicio al Ciudadano:** La Administración Municipal impulsará la incorporación de información, trámites y procedimientos a la Administración Electrónica para posibilitar la consecución más eficaz de los principios constitucionales de transparencia administrativa, proximidad y servicio a los ciudadanos
- **Principio de simplificación administrativa:** La Administración Municipal, con el objetivo de alcanzar una simplificación e integración de los procesos, procedimientos y trámites administrativos, así como de mejorar el servicio al ciudadano, aprovechará la eficiencia que comporta la utilización de técnicas de Administración Electrónica, en particular eliminando todos los trámites o actuaciones que se consideren no relevantes y rediseñando los procesos y los procedimientos administrativos, de acuerdo con la normativa de aplicación, utilizando al máximo las posibilidades derivadas de las tecnologías de la información y la comunicación.
- **Principio de impulso de los medios electrónicos:** La Administración Municipal, en cumplimiento de lo dispuesto en el apartado 3 del artículo 70 bis de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, impulsará de forma preferente el uso de los medios electrónicos en el conjunto de sus actividades y, en especial, en las relaciones con los ciudadanos. La Administración Municipal podrá establecer incentivos para fomentar la utilización de los medios electrónicos entre los ciudadanos, en los términos establecidos en la presente Ordenanza.
- **Principio de neutralidad tecnológica e interoperabilidad:** La Administración Municipal garantizará la realización de las actuaciones reguladas en esta Ordenanza con independencia de los instrumentos tecnológicos utilizados, así como la adopción de los estándares de interoperabilidad para que los sistemas de información utilizados por ella sean compatibles y se reconozcan con los de los ciudadanos y los de otras administraciones, siempre de acuerdo a lo que reglamentariamente se apruebe en cada momento dentro del Esquema Nacional de Interoperabilidad.
- **Principio de confidencialidad, seguridad y protección de datos:** La Administración Municipal, en el impulso de la Administración Electrónica, garantizará la protección de la confidencialidad y seguridad de los datos de los ciudadanos, de conformidad con los términos definidos en la normativa sobre protección de datos, en el Esquema Nacional de Seguridad y en las demás normas relativas a la protección de la confidencialidad.
- **Principio de gratuidad:** La Administración no podrá exigir contraprestación económica adicional derivada del empleo de medios electrónicos informáticos y telemáticos en sus relaciones con la ciudadanía.
- **Principio de participación:** La Administración Municipal promoverá el uso de los medios electrónicos en el ejercicio de los derechos de participación, en especial el derecho de petición, los derechos de audiencia e información pública, la iniciativa ciudadana, las consultas y la presentación de avisos, quejas, reclamaciones y sugerencias.
- **Principio de accesibilidad y usabilidad:** La Administración Municipal garantizará el uso de sistemas sencillos que permitan obtener información de interés ciudadano de manera rápida, segura y comprensible. La Administración Municipal potenciará el uso de criterios unificados en la búsqueda y visualización de la información que permitan de la mejor manera la difusión informativa, siguiendo los criterios y los estándares internacionales y europeos de accesibilidad y tratamiento documental. La Administración Municipal pondrá a disposición de los

ciudadanos con discapacidades o con especiales dificultades los medios necesarios para que puedan acceder, en condiciones de igualdad, a la información administrativa a través de medios electrónicos, siguiendo los criterios y estándares generalmente reconocidos.

- **Principio de exactitud de la información y facilitación de medios:** La Administración Municipal garantizará, en el acceso a la información por medios electrónicos, la obtención de documentos con el contenido exacto y fiel al equivalente en soporte papel o en el soporte en que se haya emitido el documento original. La disponibilidad de la información en formato electrónico no impedirá o dificultará la atención personalizada en las oficinas públicas o por otros medios tradicionales.
- **Principio de no discriminación por razón del uso de medios electrónicos:** El uso de los medios electrónicos no podrá comportar ninguna discriminación o perjuicio para los ciudadanos que se relacionen con la Administración Municipal a través de otros medios, todo ello sin perjuicio de las medidas dirigidas a incentivar la utilización de medios electrónicos.
- **Principio de voluntariedad:** Los sistemas de comunicación telemática con la Administración municipal sólo se podrán configurar como obligatorios y exclusivos en aquellos casos en que una norma con rango legal así lo establezca, en las relaciones interadministrativas, en las relaciones jurídico-tributarias y en las relaciones de sujeción especial, de conformidad con las normas jurídicas de aplicación.
- **Principio de trazabilidad de los procedimientos y documentos administrativos:** La Administración Municipal llevará a cabo las acciones necesarias para establecer sistemas y procedimientos adecuados y comprensibles de trazabilidad, que permitan a los ciudadanos conocer en todo momento, y a través de medios electrónicos, las informaciones relativas al estado de la tramitación y el historial de los procedimientos y documentos administrativos, sin perjuicio de la aplicación de los medios técnicos necesarios para garantizar la intimidad y la protección de los datos personales de las personas afectadas.
- **Principio de intermodalidad de medios:** La Administración Municipal promoverá las medidas necesarias para garantizar que los procedimientos iniciados por un medio se puedan continuar por otro distinto, siempre y cuando se asegure la integridad y seguridad jurídica del conjunto del procedimiento.
- **Principio de cooperación y colaboración interadministrativas:** Con el objetivo de mejorar el servicio al ciudadano y la eficiencia en la gestión de los recursos públicos, el Ayuntamiento impulsará la firma, con el resto de las Administraciones Públicas, de todos aquellos convenios y acuerdos que sean necesarios para hacer posibles y aplicables las previsiones incluidas en esta Ordenanza, en particular y, entre otros, los que tengan por objeto la fijación de estándares técnicos y el establecimiento de mecanismos para intercambiar y compartir información, datos, procesos y aplicaciones. En especial, la Administración Municipal garantizará la interoperabilidad de los sistemas y soluciones adoptados, así como la prestación conjunta de servicios a los ciudadanos cuando ello fuese posible.
- **Principio de acceso de las demás Administraciones Públicas y disponibilidad limitada:** La Administración Municipal facilitará el acceso de las demás Administraciones Públicas a los datos en soporte electrónico que tenga sobre los interesados y especificará las condiciones, los protocolos y los criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad e integridad. La disponibilidad de los datos mencionados en el apartado anterior se limitará, estrictamente, a los que las Administraciones Públicas requieran, en el ejercicio de sus funciones, para la tramitación y resolución de los procedimientos que sean de su competencia. El acceso a dichos datos estará condicionado al hecho de que el interesado haya dado su consentimiento o que una norma con rango legal así lo prevea.

■ **TÍTULO I. De los derechos de la ciudadanía en relación a la administración electrónica y del catálogo de servicios electrónicos**

■ **Capítulo 1º. De los derechos de la ciudadanía en relación a la administración electrónica**

■ ■ **Artículo 5. Derechos de la ciudadanía**

1. Se reconoce a la ciudadanía el derecho a relacionarse con la Administración Municipal mediante la utilización de medios electrónicos, en los términos fijados en la legislación vigente. Dicho reconocimiento se hace extensible al ejercicio efectivo de los derechos que reconoce a los ciudadanos 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 de aquellos derechos relativos a la obtención de todo tipo de informaciones, la realización de consultas, la presentación de alegaciones, la formulación de solicitudes y pretensiones, la realización de pagos y transacciones, y la oposición a las resoluciones y actos administrativos que les afecten.
2. Además, la ciudadanía tiene en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la legislación vigente y en la presente Ordenanza, los siguientes derechos:
 - a. A elegir, de entre aquellos que en cada momento se encuentren disponibles para cada procedimiento, el canal a través del cual relacionarse por medios electrónicos con la Administración Municipal.
 - b. A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán, en la medida en que los avance técnicos así lo permitan, 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 ofertados por la Administración Municipal y sus Organismos Públicos.
 - 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 los procedimientos en los que tengan la condición de interesado.
 - f. A la conservación en formato electrónico por la Administración Municipal de los documentos electrónicos que formen parte de un expediente.
 - g. A obtener los medios de tramitación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para la realización de cualquier trámite electrónico con la Administración Municipal.

- h. A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de la Administración Pública.
 - i. A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración Municipal.
 - j. A la calidad de los servicios públicos prestados por medios electrónicos.
 - k. A elegir las aplicaciones o sistemas para relacionarse con la Administración Municipal, siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por la ciudadanía.
3. En particular, en los procedimientos relativos al establecimiento de actividades de servicios, la ciudadanía tiene derecho a obtener la siguiente información a través de medios electrónicos:
- 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 de las asociaciones y organizaciones profesionales relacionadas con las mismas.
 - c. Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios y las vías de recurso en caso de litigio entre cualesquiera autoridades competentes, prestadores y destinatarios.

■ ■ Artículo 6. Medios de acceso a los servicios electrónicos

1. La Administración Municipal garantizará el acceso de la ciudadanía a los servicios electrónicos proporcionados en el ámbito de su competencia a través de un sistema de varios canales que contará, al menos, con los siguientes medios:
- a. Las oficinas de atención presencial que se determinen, las cuales pondrán a disposición de la ciudadanía de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en esta Ordenanza, 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 distintos Servicios y Organismos Públicos y disponibles para toda la ciudadanía a través de redes de comunicación.

El punto de acceso general a través del cual la ciudadanía puede, en sus relaciones con la Administración Municipal, acceder a toda la información y a los servicios disponibles será el siguiente: www.irun.org
 - c. Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a la ciudadanía el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores.

■ ■ Artículo 7. Fomento de los medios electrónicos y eliminación de la brecha digital

1. La Administración municipal podrá adoptar medidas dirigidas a fomentar que la ciudadanía realice determinadas solicitudes, procedimientos y trámites administrativos mediante la utilización de medios electrónicos, cuando esta posibilidad estuviese habilitada. En este sentido, la Administración municipal podrá establecer en sus Ordenanzas Fiscales bonificaciones y exenciones en los tributos que graven dichas actuaciones, dentro del

margen de actuación que, en este sentido, el ordenamiento vigente permite a las Corporaciones Locales. Las citadas bonificaciones y exenciones fiscales estarán fundamentadas en la eficiencia que comporta la utilización de técnicas de Administración Electrónica, así como en el consiguiente ahorro producido en los recursos financieros empleados por la Administración municipal en la tramitación de estas actuaciones mediante la utilización de medios electrónicos.

2. La Administración Municipal adoptará las medidas oportunas para que los colectivos más desfavorecidos, y aquellos ciudadanos con discapacidades o con especiales dificultades económicas, sociales o culturales, cuenten con los medios necesarios para poder acceder, en condiciones de igualdad, a los servicios municipales ofertados a través de medios electrónicos. Entre estas medidas podrá contemplarse la impartición de formación gratuita en materia de tramitación administrativa por medios electrónicos, abierta a todos los ciudadanos empadronados en la ciudad, así como la habilitación de terminales de acceso gratuito a la sede electrónica general, a lo largo de diferentes puntos de la ciudad.
3. En todo caso, se garantizará que la pertenencia a dichos colectivos o la posesión de cualquier dificultad añadida no comporte discriminación o perjuicio alguno para los mismos a la hora de acceder a los servicios electrónicos de competencia municipal, permitiéndose, en la medida de lo posible, la posibilidad de utilización de medios o canales alternativos a los electrónicos cuando aquéllos existiesen.

■ ■ Artículo 8. Transmisiones de datos entre Administraciones Públicas

1. Para un eficaz ejercicio del derecho reconocido en el artículo 5.2 b), la Administración Municipal facilitará el acceso a las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se hallen 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 establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos e Carácter Personal y su normativa de desarrollo.
2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a la ciudadanía por parte de las restantes Administraciones Públicas para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. Se exigirá, igualmente, que el acceso a los datos de carácter personal cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, o que una norma con rango de ley así lo autorice.
3. A los efectos de lo dispuesto en este artículo, la Administración Municipal podrá suscribir los oportunos convenios con otras Administraciones Públicas para garantizar la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas, promoviendo el reconocimiento mutuo de los documentos electrónicos y de los medios de identificación y autenticación que se ajusten a lo dispuesto legalmente. En todo caso, estas relaciones de cooperación se basarán en los principios de servicio al ciudadano y de simplificación administrativa.

■ **Capítulo 2º. Del catálogo de trámites, servicios y procedimientos electrónicos**

■ ■ **Artículo 9. Aprobación de Manuales de Procedimiento en materia de gestión electrónica**

1. Los Servicios municipales competentes fijarán, de común acuerdo con las Áreas funcionales afectadas y previo informe de los Servicios Jurídicos, los procedimientos a seguir para cada uno de los trámites de gestión o de información susceptibles de realizarse por medios electrónicos, en la materia que por contenido funcional les corresponda. Una vez fijados los procedimientos, se acometerá la aprobación del correspondiente Manual mediante resolución de la Alcaldía.
2. El manual de procedimiento determinará los documentos y formatos que tendrán entrada en el registro telemático, así como sus condiciones de funcionamiento. Reflejará, igualmente, los requisitos jurídicos o técnicos que las disposiciones impongan a los proyectos, actuaciones o solicitudes que los ciudadanos se propongan realizar electrónicamente.
3. El catálogo de trámites, servicios y procedimientos electrónicos estará a disposición del público en la sede electrónica general del Ayuntamiento de Irun, así como en el Servicio de Atención Ciudadana (S.A.C.)

■ ■ **Artículo 10. Referentes de Área**

Para garantizar la adecuada coordinación de los Servicios citados en el artículo anterior con las Áreas funcionales del Ayuntamiento, al objeto de prestar el mejor servicio al ciudadano, existirá la figura del Referente de Área que tendrá como funciones las siguientes:

- a. Servir de interlocutor o puente entre los Servicios citados en el artículo anterior y el Área correspondiente, ofreciendo el apoyo necesario cuando sea requerido.
- b. Proponer modificaciones y ampliaciones en el catálogo de trámites y procedimientos electrónicos, en aquellos que competencialmente correspondan a su Área.
- c. Mantener informados a los Servicios municipales competentes sobre todas las actuaciones del Área que tengan repercusión de cara al ciudadano, tales como el estado de tramitación de los procedimientos, quejas y reclamaciones, anuncios, campañas, y en general de cuantas actividades desarrolle el Área.
- d. Velar y coordinar las actuaciones necesarias de respuesta dentro de su Área por las demandas del ciudadano presentadas a través de la página Web del Ayuntamiento o de cualquier otra sede electrónica.
- e. Controlar el correcto cumplimiento de los Manuales de procedimiento aprobados, y que por contenido funcional le corresponda.

■ **TÍTULO II. Del régimen jurídico de la administración electrónica**

■ **Capítulo 1º. De la sede electrónica**

■ ■ **Artículo 11. Las Sedes Electrónicas**

1. Las sedes electrónicas son todas aquellas direcciones electrónicas disponibles para la ciudadanía a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a un órgano, área, entidad administrativa u organismo público del Ayuntamiento de Irun en el ejercicio de sus competencias.

2. El Ayuntamiento de Irun y los diferentes organismos públicos del mismo velarán por la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de cada sede electrónica.
3. Las sedes electrónicas se establecerán, previo informe de los Servicios municipales competentes, a solicitud del órgano, unidad u organismo interesado, con sujeción a los principios de publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. Se garantizará, en todo caso, la identificación del titular de la sede, así como la disponibilidad de medios para la formulación de sugerencias y quejas.
4. Cuando resulte necesario, se habilitarán en las distintas sedes electrónicas sistemas que permitan el establecimiento de comunicaciones seguras.
5. La publicación, en las sedes electrónicas que sean titularidad del Ayuntamiento de Irun y de sus organismos públicos, 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 la ciudadanía.
6. En el Ayuntamiento de Irun se mantendrá un registro actualizado de sedes electrónicas, características, condiciones de uso y titular de las mismas.

■ ■ Artículo 12. La Sede Electrónica General

1. Se establece como sede electrónica general de la Administración municipal el punto de acceso electrónico general, www.irun.org. En esta sede, se pondrá a disposición de la ciudadanía la relación de servicios y el modo de acceso a los mismos, debiendo mantenerse coordinado con los restantes puntos de acceso electrónico de la Administración municipal y sus Organismos Públicos, hacia los que existirá un enlace directo.
2. De conformidad con lo dispuesto en la Disposición Adicional Segunda de la presente Ordenanza, la sede electrónica general estará disponible en euskera y castellano, pudiendo incluirse informaciones en otros idiomas cuando ello se considere de interés general.
3. Los Servicios Generales del Ayuntamiento de Irun se responsabilizarán de la sede electrónica general de la Administración municipal, y a ellos corresponderá su gestión y administración, sin perjuicio de las competencias que, con respecto a su contenido, pudieran poseer otras Áreas y Servicios municipales.

■ ■ Artículo 13. Publicación electrónica del tablón de anuncios o edictos

1. Los actos y comunicaciones que, en virtud del procedimiento administrativo, norma jurídica o resolución judicial, deban publicarse en tablón de anuncios o edictos, se publicarán también en la sede electrónica general. En los casos en que se considere oportuno y legalmente posible, la publicación en tablón de anuncios o edictos podrá ser sustituida por la publicación en la sede electrónica general, advirtiéndose de ello en el espacio físico actualmente destinado a Tablón de Anuncios.
2. El tablón de anuncios electrónico se podrá consultar, a través de la sede electrónica general, a la que se podrá acceder desde los diferentes terminales instalados por el Ayuntamiento de Irun en diferentes puntos de la Ciudad. En todo caso, se garantiza el acceso de toda la ciudadanía y la ayuda necesaria para su consulta efectiva, no

requiriéndose ningún mecanismo especial de acreditación de la identidad del ciudadano salvo en los casos en que, de conformidad con lo dispuesto en el artículo 61 de la LRJ-PAC, se pretenda el acceso al contenido íntegro de un acto publicado someramente en el tablón de anuncios electrónico, por parte de quienes acrediten interés legítimo en el conocimiento del mismo.

3. El tablón de anuncios electrónico estará disponible en la sede electrónica general de la Administración municipal las 24 horas del día, todos los días del año. Cuando por razones técnicas se prevea que el tablón de edictos electrónico puede no estar operativo, se deberá informar de ello a los usuarios con la máxima antelación posible, indicando cuáles son los medios alternativos de consulta del tablón que estén disponibles.
4. El tablón de edictos electrónico dispondrá de los sistemas y mecanismos que garanticen la autenticidad, la integridad y la conservación de su contenido, en los términos previstos en el artículo 45.5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En especial, a los efectos del cómputo de los plazos que corresponda, se establecerá el mecanismo que garantice la constatación de la fecha y hora de publicación de los edictos.

■ **Capítulo 2º. De la función de información y su difusión por medios electrónicos**

■ ■ **Artículo 14. Información general**

A través de la sede electrónica general y sin necesidad alguna de identificación, la ciudadanía tendrá acceso libre y permanente a la siguiente información:

- a. La identificación, fines, competencia, estructura, funcionamiento, localización y responsables de servicios, organismos y unidades administrativas que componen la Administración municipal y sus organismos autónomos.
- b. La referida a los requisitos jurídicos o técnicos que las disposiciones impongan a los proyectos, actuaciones o solicitudes que los ciudadanos se propongan realizar.
- c. Un catálogo general de los servicios que presta la Administración municipal, además de la información relativa a la tramitación de procedimientos, a los servicios públicos y prestaciones, así como a cualesquiera otros datos que aquellos tengan necesidad de conocer en sus relaciones con las Administraciones públicas, complementada con la relativa a servicios y trámites extramunicipales que se conozcan de mayor interés para el ciudadano.

A modo de ejemplo, la Administración Municipal hará pública la siguiente información:

- Un catálogo general de servicios municipales.
- Los acuerdos de los órganos de gobierno, sin perjuicio de la ocultación de los datos de carácter personal que aquéllos pudieran contener.
- Las Ordenanzas y demás normativa municipal, incluidas las Ordenanzas Fiscales.
- El presupuesto municipal y las cuentas generales aprobadas.
- Las figuras de planeamiento urbanístico.
- Los anuncios de información pública.

- Los procedimientos de contratación administrativa, a través del perfil de contratante establecido en el artículo 42 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.
 - Los procedimientos de concesión de subvenciones.
 - Los procedimientos de selección de personal.
 - Los impresos y formularios de los trámites y procedimientos municipales.
 - El callejero municipal
- d. El conocimiento del procedimiento, o parte del mismo que se determine, en información pública, pudiendo realizar los ciudadanos las alegaciones que consideren oportunas.
- e. Procedimientos de participación ciudadana
- f. El buzón de avisos, quejas y sugerencias.
- g. Asuntos o cuestiones de interés general para los ciudadanos, incluida la que pueda contribuir a una mejor calidad de vida de los ciudadanos y tenga una especial incidencia social, por ejemplo en los ámbitos de sanidad, salud, cultura, educación, servicios sociales, medio ambiente, transportes, comercio, deportes y tiempo libre.

■ ■ Artículo 15. El Boletín de Información Municipal

El Ayuntamiento de Irun, a través de su sede electrónica general, pondrá a disposición de la ciudadanía en general, para su conocimiento y consulta, el Boletín de Información Municipal, que incluirá un extracto de todos los acuerdos y resoluciones adoptados y, además, cuando sea obligatoria la divulgación conforme a la Ley 7/1985 de 2 de abril, Reguladora de las Bases del Régimen Local, y su normativa de desarrollo, o merezcan ser divulgados, por tratarse de adopción de medidas excepcionales, llamamientos al vecindario, referencias históricas y anales locales y provinciales.

■ ■ Artículo 16. Información particular

1. Se entiende por información particular la concerniente al estado o contenido de los procedimientos en tramitación, y a la identificación de las autoridades y personal al servicio de la Administración bajo cuya responsabilidad se tramiten aquellos procedimientos
2. Aquellas personas a las que, previa acreditación mediante los medios que se establecen en el siguiente capítulo, se les reconozca su condición de interesado conforme a lo previsto en el artículo 31 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrán emplear medios electrónicos para:
 - a. Obtener información en cualquier momento sobre el estado de la tramitación del procedimiento
 - b. Acceder a los documentos que obren en el expediente.
 - c. Participar en el trámite de audiencia a fin de alegar y presentar los documentos y justificaciones que estimen pertinentes.

■ **Capítulo 3º. De la identificación y autenticación**

■ ■ **Artículo 17. Formas de identificación y autenticación**

1. La ciudadanía podrá emplear los siguientes sistemas de firma electrónica para relacionarse telemáticamente con la Administración municipal:
 - a. Los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas. Su régimen de utilización y efectos se regirá por su normativa reguladora.
 - b. Los sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido. La relación y características de los sistemas de firma electrónica avanzada admitidos en cada momento para la tramitación electrónica estará disponible en la sede electrónica general, especificándose en cada caso los prestadores que expiden dichos certificados electrónicos.
2. Por su parte, la Administración municipal podrá utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que emita:
 - 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, que deberán ser solicitados por el Secretario del Ayuntamiento al proveedor del sistema.
 - b. Sistemas de firma electrónica para la actuación administrativa automatizada, que deberán ser solicitados por el Secretario del Ayuntamiento al proveedor del sistema previo cumplimiento de lo dispuesto en el artículo 35: sello electrónico basado en certificado electrónico y código seguro de verificación. La relación de los sellos electrónicos utilizados por la Administración municipal, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, será pública y se podrá acceder a ella en la sede electrónica general. Además, mediante el acceso a la sede electrónica correspondiente, se permitirá la comprobación de la integridad de los documentos que se generen electrónicamente en prueba o confirmación de aquello que conste en los registros municipales, a través de un código seguro de verificación.
 - c. Firma electrónica del personal al servicio de la Administración municipal y sus organismos públicos. A estos efectos, el Ayuntamiento de Irun proveerá a su personal de sistemas de firma electrónica que identifiquen de forma conjunta al titular del puesto o cargo y a la Administración u órgano en la que presta sus servicios, que deberán ser solicitados por el Secretario del Ayuntamiento al proveedor del sistema. En caso necesario, dicho personal podrá utilizar la firma electrónica basada en el Documento Nacional de Identidad, a los efectos de lo dispuesto en este precepto.
 - d. Intercambio electrónico de datos en entornos cerrados de comunicación. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores. Se garantizará, a estos efectos, la seguridad del entorno y la protección de los datos transmitidos.

Mediante resolución de la Alcaldía se deberá aprobar, dentro de la Administración municipal, la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar. Cuando se realice el intercambio con otra Administración Pública, se deberán fijar previamente las condiciones y garantías por las que se regirá la transmisión, en el oportuno convenio al efecto.

■ ■ Artículo 18. La tarjeta ciudadana

1. El Ayuntamiento de Irun gestionará con proveedores autorizados la emisión gratuita, para todos los ciudadanos que así lo solicitaren, de una tarjeta ciudadana personal e intransferible que, además de otros usos ciudadanos que se le pudieran añadir para el disfrute de determinados servicios municipales, contendrá un certificado de firma electrónica reconocida que permita relacionarse electrónicamente con la Administración municipal.
2. Esta tarjeta ciudadana podrá contener otros elementos técnicos para la identificación de su titular, tales como chips de proximidad (mifare), de cara al acceso de aquél a determinados servicios y trámites municipales que no requieran una identificación mediante firma electrónica reconocida.
3. La solicitud de la tarjeta se efectuará de forma directa, por parte de la persona solicitante o por su representante previa acreditación de su identidad, en las dependencias del Servicio de Atención Ciudadana y en cualquier otra que se pudiera establecer al efecto, previa información en la sede electrónica general. En el momento de recoger la tarjeta, la persona interesada o su representante previa acreditación de su identidad, firmarán el documento de determinación de las condiciones uso de la misma que incluirá, en su caso, las condiciones de uso de los otros servicios que se presten con la tarjeta y que, en su regulación, prevean unas condiciones de uso específicas.

■ ■ Artículo 19. Interoperabilidad de la identificación y autenticación por medio de certificados electrónicos

1. El Ayuntamiento de Irun admitirá como válidos para relacionarse electrónicamente con el mismo aquellos certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación, siempre que dicho prestador de servicios de certificación ponga a disposición del primero la información que resulte precisa en condiciones que resulten tecnológicamente viables, y sin que suponga coste alguno para aquél.
2. Aquellos sistemas de firma electrónica utilizados o admitidos por parte de alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior, podrán ser admitidos por el Ayuntamiento de Irun únicamente si así se acordase con dichas Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad.
3. El Ayuntamiento de Irun habilitará los mecanismos necesarios para verificar el estado de revocación y la firma de todos los certificados admitidos en su ámbito de competencia.

■ ■ Artículo 20. Identificación y autenticación por parte de funcionarios públicos

1. En los supuestos en los que para la realización de cualquier tramitación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de firma electrónica de los establecidos en este capítulo de los que aquél no disponga, tal identificación o autenticación podrá ser válidamente realizada por funcionarios públicos, previamente facultados para ello por el secretario del Ayuntamiento, mediante el uso del sistema de firma electrónica del que estén dotados. Para ello, el ciudadano deberá identificarse y prestar consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.
2. El Ayuntamiento mantendrá actualizado un registro de funcionarios habilitados para la identificación o autenticación regulada en este artículo.

■ ■ Artículo 21. Representación para la tramitación electrónica

1. Los ciudadanos podrán actuar por medio de representantes en los procedimientos y trámites administrativos que se realicen frente a la Administración Municipal por medios electrónicos, de acuerdo con lo que prevé la legislación general y lo que establece esta Ordenanza. Así, cualquier persona física con capacidad de obrar plena y en posesión de un certificado de firma electrónica reconocida, podrá representar a otras personas, físicas o jurídicas, en los procedimientos y trámites administrativos que se realicen, por medios electrónicos, ante el Ayuntamiento de Irun. En estos supuestos, se presumirá la validez de las actuaciones realizadas, condicionada a la acreditación de la representación, que podrá ser requerida en cualquier momento por el Ayuntamiento de Irun.
2. Las personas físicas que pretendan actuar ante el Ayuntamiento de Irun en nombre y representación de otras personas físicas o jurídicas, acreditarán la representación por los siguientes medios:
 - a. Documento público o privado con firma notarialmente legitimada, cuando la persona representada sea una persona jurídica o una persona física incapacitada judicialmente (representación legal)
 - b. Por la comparecencia personal de la persona representada y del representante, ante el órgano administrativo competente que se determine, cuando la persona representada sea una persona física con capacidad de obrar plena (representación voluntaria)
3. Sin perjuicio de lo dispuesto en el punto anterior, el Ayuntamiento podrá constituir un censo de representantes para la tramitación telemática, constituido por los representantes legales de las personas jurídicas que, por razón de su actividad profesional, realicen tramitaciones administrativas con el Ayuntamiento de Irun en nombre de terceras personas. Estas personas podrán, una vez formen parte del censo de representantes, dar de alta representaciones de personas físicas concretas, una vez hayan sido autorizadas por éstas en el documento oportuno que se habilite al efecto.
4. La representación podrá otorgarse con carácter general para todos los trámites que los relacionen con el Ayuntamiento de Irun, o únicamente para uno o varios trámites, según conste en la acreditación presentada o se haya manifestado, por parte del representado, en el acto de otorgamiento de la representación.
5. La representación otorgada podrá tener carácter temporal o indefinido, siendo válida en este último caso hasta su posterior revocación por parte del representado.

■ ■ Artículo 22. Registro de representantes para la tramitación electrónica

1. El Ayuntamiento de Irun contará con un Registro de Representantes para la Tramitación Electrónica, que recogerá todas las inscripciones válidamente formuladas por parte de los interesados.
2. El órgano competente aprobará un modelo normalizado para la solicitud de alta, modificación o baja del Registro de Representaciones para la Tramitación Electrónica, cuya cumplimentación será requisito imprescindible para la inscripción de la representación en el citado Registro, y que recogerá el plazo de duración de la inscripción de la representación y el alcance de la misma.
3. Las solicitudes de alta, modificación o baja del Registro de Representaciones para la Tramitación Electrónica deberán resolverse expresamente por el Ayuntamiento de Irun en el plazo de tres meses, entendiéndose estimadas en caso de no recaer resolución expresa en dicho plazo.

■ ■ Artículo 23. Pluralidad de interesados

Cuando en una solicitud telemática haya más de un interesado, ésta tendrá que ser firmada electrónicamente por todos ellos, y las actuaciones se realizarán con el que se haya señalado expresamente o, en su defecto, con el interesado que aparezca como primer firmante.

■ ■ Capítulo 4º. *Del registro telemático*

■ ■ Artículo 24. El registro telemático

1. Mediante la presente disposición se crea en el Ayuntamiento de Irun un registro telemático, auxiliar del registro general en los términos previstos en el artículo 38.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Dicho registro telemático estará habilitado para la recepción y remisión de documentos electrónicos normalizados, integrándose con todos los efectos en el Registro General del Ayuntamiento de Irun.
2. Únicamente se podrán presentar por medios electrónicos aquellas solicitudes, comunicaciones y escritos de los interesados que, en formato electrónico normalizado, previamente se hayan determinado y que oportunamente se recogerán en el catálogo de trámites y procedimientos electrónicos a disposición del público en la sede electrónica general del Ayuntamiento de Irun, así como en el Servicio de Atención Ciudadana (S.A.C.). Podrán acompañarse los documentos electrónicos que se consideren oportunos, siempre que cumplan con los estándares de formato y requisitos de seguridad que se determinen en los esquemas nacionales de interoperabilidad y de seguridad.
3. El acuerdo de creación de cualquier registro telemático se publicará en el Boletín Oficial de Gipuzkoa, y su texto íntegro estará disponible para consulta en la sede electrónica general. Las disposiciones de creación de estos registros telemáticos especificarán el órgano o unidad administrativa responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles. En cualquier caso, no será de aplicación al registro telemático lo dispuesto en el artículo 48.5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
4. El acceso al registro telemático de entrada se podrá realizar durante las 24 horas, todos los días del año. La fecha y hora de entrada se acreditará mediante el sellado de tiempo proporcionado por una de las entidades proveedoras de los sistemas de firma electrónica avanzada que se admitan, sellado que se realizará en el menor tiempo técnicamente posible desde el momento de la recepción de la solicitud completa en la sede electrónica del Ayuntamiento y que constituirá la fecha y hora a tener en cuenta para el cómputo de plazos legales. A efectos de cómputo de plazo, la recepción en un día inhábil se entenderá efectuada en la primera hora del primer día hábil siguiente, sin perjuicio de la existencia de una norma que permitiese expresamente la recepción en día inhábil. En todo caso, el registro telemático se registrará por la fecha y la hora oficiales del servidor de sellado de tiempo de la sede electrónica de acceso, que contará con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.
5. El registro telemático de salida estará operativo las 24 horas, todos los días del año. La fecha de salida se acreditará mediante un servicio de consignación electrónica de fecha y hora, coincidiendo con la fecha en que, de acuerdo con lo establecido para la notificación electrónica, se inicia el proceso de depósito de la notificación en el buzón de la Web personal del interesado que se define en el artículo 36 de la presente Ordenanza. A los efectos del cómputo de plazos, la anotación de la salida de un escrito o comunicación en el registro telemático en un día

inhábil se entenderá realizada en la primera hora del primer día hábil siguiente, momento en el que se iniciará formalmente el proceso de notificación de la misma salvo que una norma permita expresamente el envío en día inhábil.

6. El registro telemático de entrada emitirá automáticamente un justificante de la recepción de los documentos electrónicos presentados por los interesados, en el cual se dará constancia de la fecha y hora en que se inscribe, y número de orden que le haya correspondido, garantizando siempre la integridad y el no repudio de los documentos aportados. En cualquier caso, la Administración municipal podrá reconvertir el formato del documento que haya recibido cuando lo considere necesario para su lectura, almacenamiento y archivo, sin que pueda alterarse el contenido sustantivo de aquél.
7. La disponibilidad del registro telemático únicamente podrá interrumpirse cuando concurren causas justificadas de mantenimiento técnico u operativo, y únicamente por el tiempo imprescindible para su reparación. Cuando por razones técnicas el registro no esté operativo, se deberá informar de ello a los usuarios con la máxima antelación posible y mientras dure esta situación. En los supuestos de interrupción no anunciada del funcionamiento del registro telemático, el usuario visualizará un mensaje advirtiéndole de tal circunstancia.

■ ■ Artículo 25. Registro externo telemático

Mediante la suscripción del oportuno convenio de colaboración, se podrá habilitar el registro telemático para la recepción de solicitudes, escritos y comunicaciones de la competencia de otras Administraciones Públicas.

■ ■ Artículo 26. Días inhábiles para el registro telemático

1. Serán considerados días inhábiles para el registro telemático y para los usuarios de éste únicamente los así declarados para todo el territorio nacional en el calendario anual de días inhábiles, y los así declarados en el ámbito territorial de la Comunidad Autónoma del País Vasco y en el municipio de Irun, como fiesta local.
2. Los días inhábiles de cada año concreto figurarán en la sede electrónica general.

■ Capítulo 5º. *De las comunicaciones electrónicas*

■ ■ Artículo 27. Comunicaciones electrónicas

1. Con el fin de garantizar el derecho del ciudadano a relacionarse con la Administración municipal, se garantizará la comunicación por vía telemática con plenos efectos jurídicos al amparo de lo que establece la presente Ordenanza.
2. Excepto en los casos en los que una norma con rango de ley prescriba la utilización de un medio no electrónico, cualquier ciudadano podrá elegir, en todo momento, la manera de comunicarse con la Administración municipal por medios electrónicos. La opción de comunicarse por unos u otros medios no vinculará al ciudadano, pudiendo éste optar, en cualquier momento, por un medio distinto del inicialmente elegido.
3. La Administración municipal utilizará medios electrónicos en sus comunicaciones con los ciudadanos únicamente en los casos en los que aquéllos lo hubiesen solicitado o consentido expresamente.

4. Se presumirán válidas las comunicaciones a través de medios electrónicos 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.
5. La Administración municipal velará por la seguridad e integridad de las comunicaciones realizadas por medios electrónicos, estableciendo las medidas apropiadas en función del carácter de los datos objeto de aquéllas.
6. La Administración municipal informará de aquellos medios electrónicos al alcance de la ciudadanía para el ejercicio del derecho a comunicarse con aquélla, en su sede electrónica general.

■ ■ **Artículo 28. Obligatoriedad del uso de medios electrónicos para la realización de determinadas comunicaciones**

1. La presente ordenanza habilita a la Alcaldía para que, a través de la oportuna resolución, determine la obligatoriedad de comunicarse con la Administración municipal mediante el uso exclusivo de medios electrónicos, siempre que los destinatarios o remitentes afectados sean personas jurídicas, que las comunicaciones se produzcan al margen de los procedimientos administrativos y que el objeto de las comunicaciones no pueda implicar, en ningún caso, restricción o pérdida de derechos para ninguna de las partes. Fuera de estos casos, será precisa la aprobación de una disposición de carácter general para establecer la obligatoriedad de la utilización de estos medios para comunicarse con la Administración municipal.
2. El Ayuntamiento de Irun potenciará el uso de medios electrónicos en sus comunicaciones con otras Administraciones Públicas, sin perjuicio de lo dispuesto en el artículo 8 de la presente Ordenanza respecto de la posibilidad de acordar el acceso electrónico a los datos que obren en poder de otras Administraciones.

■ **TÍTULO III. De la gestión electrónica de los procedimientos**

■ **Capítulo 1º. De los principios de actuación en la gestión electrónica de los procedimientos**

■ ■ **Artículo 29. Aplicación de medios electrónicos en la gestión de procedimientos**

1. La aplicación de medios electrónicos a los procesos de trabajo y a la gestión de los procedimientos y de la actuación administrativa se regirá, en todo caso, por criterios de eficiencia, servicio al ciudadano y simplificación administrativa.
2. La gestión electrónica de la actividad administrativa municipal respetará siempre la titularidad y el ejercicio de la competencia por parte de la Administración, órgano o entidad que la tuviere atribuida, así como el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad.

■ ■ **Artículo 30. Requisitos previos para la aplicación de medios electrónicos en la gestión**

1. La aplicación de medios electrónicos a la gestión de los procedimientos administrativos seguirá la mecánica establecida en el artículo 9 de la presente Ordenanza, y deberá ir precedida, en todo caso, de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio a cargo del Servicio de Organización y Calidad, que deberá de ser visado por los Servicios Jurídicos del Ayuntamiento antes de su aprobación.

2. En dicho análisis se considerarán especialmente los siguientes aspectos:
 - La supresión o reducción de la documentación requerida a la ciudadanía, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regulación de su aportación al finalizar la tramitación.
 - La previsión de medios o instrumentos de participación, transparencia e información
 - La reducción de los plazos, trámites innecesarios y tiempos de respuesta
 - La racionalización de la distribución de cargas de trabajo y de las comunicaciones internas.

■ **Capítulo 2º. De la utilización de medios electrónicos en la tramitación de los procedimientos**

■ ■ **Artículo 31. Iniciación del procedimiento por medios electrónicos**

1. Los interesados podrán iniciar determinados procedimientos administrativos por medios electrónicos, derivados de los servicios municipales que se incluyan en el catálogo de trámites, servicios y procedimientos electrónicos. Para ello, deberán identificarse y autenticarse mediante los sistemas previstos en la presente Ordenanza, y acceder al portal de administración electrónica disponible en la sede electrónica general.
2. En todo caso, las solicitudes que se inicien telemáticamente deberán reunir los requisitos establecidos en el artículo 70.1 de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o normativa que la sustituya.
3. En estas solicitudes los interesados podrán incorporar copias digitalizadas de los documentos que obren en su poder, cuya fidelidad con el original garantizarán mediante la utilización de un sistema de firma electrónica avanzada. La Administración municipal podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Con carácter excepcional y sólo ante la imposibilidad de dicho cotejo, podrá requerir al interesado la exhibición del documento o de la información original.
4. La aportación de tales copias implica la autorización a la Administración municipal para que acceda y trate la información personal contenida en tales documentos.
5. En los casos que oportunamente se establezca en los Manuales de Procedimientos, la Administración municipal promoverá la sustitución de la aportación de documentos acreditativos del cumplimiento de requisitos por una declaración responsable del interesado que exprese la concurrencia de dichos requisitos y el compromiso de aportar los justificantes a requerimiento de la Administración.
6. Cuando ello se estimare oportuno para facilitar y promover su uso, los sistemas normalizados de solicitud del portal de administración electrónica podrán incluir comprobaciones automáticas de la información aportada respecto de los datos almacenados en sistemas propios o pertenecientes a otras Administraciones e, incluso, ofrecer los campos del formulario electrónico cumplimentados, en todo o en parte, con objeto de que el interesado verifique la información y, en su caso, la modifique y complete.

■ ■ Artículo 32. Instrucción del procedimiento utilizando medios electrónicos

1. El Ayuntamiento de Irun promoverá la utilización de aplicaciones y sistemas de información para la instrucción electrónica de expedientes y procedimientos, en aras a la simplificación y la eficiencia en la gestión de los mismos. Dichos sistemas 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, incorporando en dicha tramitación sistemas de firma electrónica de los citados en el artículo 17.2 c) de la presente Ordenanza cuando ello fuese posible.
2. Cuando de la instrucción electrónica de los procedimientos se deriven comunicaciones entre los órganos y unidades intervinientes a efectos de emisión y recepción de informes u otras actuaciones, se garantizará el cumplimiento de los requisitos establecidos en el artículo 27 de la presente Ordenanza.
3. Igualmente, en el caso de que en un procedimiento o actuación administrativa se contemple la posibilidad de presentación de alegaciones o la práctica del trámite de audiencia mediante el uso de medios electrónicos, la Administración municipal garantizará el cumplimiento de lo dispuesto en el artículo citado en el párrafo anterior, así como de las previsiones de la presente Ordenanza para la práctica de las notificaciones electrónicas.

■ ■ Artículo 33. Acceso de los interesados a la información sobre el estado de tramitación

1. Salvo que la normativa aplicable estableciese restricciones a esta información, los ciudadanos podrán conocer, previa identificación y autenticación por los sistemas previstos en el capítulo III del Título Segundo de la presente Ordenanza, el estado de tramitación de cualquier expediente en el que figure como titular, representante autorizado o interesado, mediante un servicio electrónico de acceso restringido al que se accederá a través del portal de administración electrónica.
2. La información sobre el estado de tramitación de los expedientes comprenderá la relación de actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados, además de un acceso *on-line* a los documentos que se generaron en cada uno de los mencionados actos de trámite.
3. Además de la información descrita en los párrafos anteriores, los ciudadanos podrán acceder a una relación de todas aquellos escritos, comunicaciones y solicitudes por ellos formuladas que hayan generado un apunte en el registro de entrada de la Administración municipal, así como de todas aquellas comunicaciones y oficios que se les hubiesen remitido desde aquella mediante la generación de un apunte en el registro de salidas.
4. En cualquier caso, la Administración municipal podrá remitir al interesado avisos sobre el estado de la tramitación, a las direcciones telemáticas de contacto que éste le haya indicado o por cualquier otro medio que lo permita.

■ ■ Artículo 34. Terminación del procedimiento por medios electrónicos

1. El acto o resolución que, mediante el uso de medios electrónicos, ponga fin a un procedimiento deberá cumplir los requisitos previstos en el artículo 89 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. La resolución de un procedimiento utilizando medios electrónicos garantizará la identidad del órgano competente mediante el empleo de alguno de los instrumentos previstos al efecto en la presente Ordenanza.
3. En el Manual de Procedimientos previsto en el artículo 9 de la presente Ordenanza podrá preverse la adopción y notificación de resoluciones de forma automatizada, cuando ello fuese posible.

■ ■ Artículo 35. Actuación administrativa automatizada

1. En caso de actuación automatizada, la Administración municipal establecerá, en el Manual de Procedimientos al que se refiere el artículo anterior, 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.
2. En dicho Manual se indicará, igualmente, el órgano municipal que deba ser considerado responsable a efectos de impugnación de acuerdos.

■ ■ Artículo 36. Práctica de la notificación por medios electrónicos

1. La Administración municipal podrá practicar la notificación por medios telemáticos siempre que los interesados, poseedores de firma electrónica reconocida, hayan manifestado la aceptación del sistema; bien por haber indicado el medio telemático como preferente para la recepción de notificaciones en su solicitud, escrito o comunicación, o bien por haber consentido expresamente su utilización, sin perjuicio de lo dispuesto en esta Ordenanza para la obligatoriedad de las comunicaciones mediante medios electrónicos.
2. Los titulares de un certificado de firma electrónica reconocida que accedan, mediante su identificación y autenticación de acuerdo a lo dispuesto en esta Ordenanza, al portal municipal de administración electrónica para la realización de cualquier tramitación, dispondrán de su propio buzón en la Web personal, que tendrá vigencia indefinida. Dicho buzón de la Web personal quedará inhabilitado, a los solos efectos de la práctica de notificaciones telemáticas, en los supuestos en los que el titular solicite expresamente su revocación o modificación, en los casos de defunción de la persona física o extinción de la personalidad jurídica, cuando una resolución administrativa o judicial ordene lo contrario o por el transcurso de tres años sin que se utilice aquél para la práctica de las notificaciones, supuesto este último en el cual le será comunicado al interesado para que pueda expresar su interés por mantener el sistema activo.
3. La notificación telemática se entenderá practicada a todos los efectos legales en el momento en que se produzca el acceso al contenido de la notificación en el buzón de la Web personal, previa incorporación de la firma electrónica del interesado. Para ello, el Ayuntamiento de Irun habrá informado anteriormente al interesado, por los medios auxiliares que se establezcan, de la existencia de una notificación en el buzón de la Web personal, procurando, en todo caso, la utilización de las nuevas tecnologías (NTIC's) para facilitar al máximo la comunicación con el interesado.

El sistema de notificación acreditará las fechas y las horas en que se produzca:

- a. El depósito de la notificación en el buzón de la Web personal del interesado.

En el caso de que, tras el depósito de la notificación en el buzón de la Web personal, hayan transcurrido diez días naturales sin acceder al contenido de la misma, ésta se enviará por correo a través del procedimiento ordinario, de acuerdo con el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, salvo que de oficio o a instancias del interesado se compruebe la imposibilidad técnica o material del acceso a su buzón de la Web personal.

- b. El acceso al contenido de la notificación.

Tras el acceso al contenido de la notificación y una vez generado el sellado de tiempo (fecha y hora), como si de un acuse de recibo se tratara, empezarán a computarse los plazos legales que la notificación disponga.

En el supuesto de que el acto que se pretende notificar conlleve aparejada la necesidad de realización de un pago por parte del administrado, y una vez que éste, previa incorporación de la firma electrónica, haya accedido al contenido de la correspondiente liquidación tributaria en su buzón de la Web personal, se entenderá notificado dicho acto desde la ejecución del citado pago.

- c. Cualquier causa técnica que imposibilite alguna de las circunstancias anteriores.
4. Durante la tramitación de los procedimientos, el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, en cuyo caso se deberá usar cualquier otro medio admitido por el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sin perjuicio de lo dispuesto en esta Ordenanza para la obligatoriedad de las comunicaciones mediante medios electrónicos.

■ ■ **Artículo 37. El Manual de Seguridad**

1. El Manual de Seguridad para la elaboración de las aplicaciones informáticas que sirvan de soporte a la tramitación telemática contendrá las medidas de seguridad de carácter general, de índole técnica y organizativa, que aseguren el cumplimiento de las garantías de autenticidad, integridad, confidencialidad, disponibilidad y conservación de la información, de conformidad con lo dispuesto en esta Ordenanza.
2. El Manual de Seguridad se aprobará por resolución de Alcaldía, fijándose en la misma cuál habrá de ser la difusión de cada una de las previsiones del mismo.

■ **Capítulo 3º. De los documentos y los archivos electrónicos**

■ ■ **Artículo 38. Documentos, certificados y volantes electrónicos**

1. La Administración municipal podrán emitir válidamente por medios electrónicos documentos, certificados y volantes electrónicos, siempre que aquéllos incorporen las firmas electrónicas necesarias a las que se refiere el artículo 17.2 de la presente Ordenanza.
2. Los procedimientos para la emisión de este tipo de documentos, certificados y volantes electrónicos deberán ser establecidos conforme a lo dispuesto por el artículo 9 de la presente Ordenanza. En cualquier caso, en los documentos electrónicos emitidos por los órganos en el ámbito de aplicación de esta Ordenanza se garantizará que la firma electrónica sólo pueda ser utilizada por los signatarios debidamente autorizados en razón de sus competencias o funciones.
3. Estos documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos -sellado de tiempo proporcionado por una de las entidades proveedoras de los sistemas de firma electrónica- cuando la naturaleza del documento así lo requiera, lo que se podrá acreditar en cualquier momento mediante el código seguro de verificación al que se refiere el apartado b) del artículo 17.2 de la presente Ordenanza.

■ ■ **Artículo 39. Copias electrónicas**

1. La Administración municipal aceptará como copias auténticas, con los efectos jurídicos previstos en el artículo 46 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, siempre que el documento electrónico original se encuentre

en poder de aquella y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento. Dicha aceptación, a salvo los requisitos señalados en este punto, se producirá con independencia de que se mantenga o no el formato original en la copia.

2. En lo que respecta a las copias realizadas por la Administración municipal mediante la utilización de medios electrónicos, cuando se trate de documentos emitidos originalmente en soporte papel por parte de la misma, tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
3. La Administración municipal, mediante el procedimiento de compulsión electrónica establecido en el siguiente artículo, podrá obtener imágenes electrónicas digitalizadas de los documentos privados aportados por la ciudadanía, con su misma validez y eficacia. Se deberá garantizar, para ello, la autenticidad, integridad y la conservación del documento imagen. La obtención de estas imágenes, en los casos en que así se determine, podrá realizarse de forma automatizada, mediante el correspondiente sellado electrónico.
4. La Administración municipal podrá aprobar, en los términos citados en el artículo 9 de la presente Ordenanza, Manuales de Procedimiento que permitan la destrucción de los documentos emitidos originalmente en papel de los que se hayan efectuado copias electrónicas de acuerdo a lo señalado en este artículo.
5. Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente, que se presenten ante la Administración municipal, tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código seguro de verificación generado electrónicamente, que permita contrastar su autenticidad mediante el acceso electrónico a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

■ ■ **Artículo 40. Compulsión electrónica de documentos y reproducción de documentos electrónicos en soporte papel**

1. La compulsión electrónica de los documentos en soporte papel se realizará mediante un procedimiento de digitalización seguro, que incluya la firma electrónica reconocida del personal al servicio de la Administración Municipal que haya realizado la compulsión y que garantice la autenticidad e integridad de la copia, sin perjuicio del empleo de otros métodos de autenticación electrónica de los previstos en el artículo 17.2 de la presente Ordenanza. Los documentos compulsados electrónicamente tendrán la consideración de copias auténticas, a los efectos de lo previsto en el artículo 46 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. La incorporación de documentos en soporte papel a los trámites y procedimientos administrativos que se hayan iniciado por vía electrónica se podrá realizar mediante la compulsión electrónica de los documentos en soporte papel.
3. Los documentos compulsados electrónicamente podrán ser válidos tanto en el procedimiento concreto para el que se ha realizado la compulsión como para cualquier otro procedimiento tramitado por la Administración Municipal.
4. Cuando un procedimiento iniciado electrónicamente no se tramite totalmente en soporte electrónico, se procederá, por parte del órgano competente, a la reproducción en soporte papel de las solicitudes, comunicaciones u otros documentos electrónicos, con el fin de continuar con la tramitación del expediente, asegurando en cualquier caso el archivo seguro de los documentos electrónicos originales.

5. En la reproducción de documentos electrónicos a copias en soporte papel, cuando no puedan reunirse los requisitos técnicos establecidos en el artículo 39.5 de la presente Ordenanza, se hará constar la diligencia del personal competente que acredite la correspondencia y la exactitud con el documento original electrónico. Estos documentos tendrán la consideración de copias auténticas, a los efectos de lo previsto en el artículo 46 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
6. Los documentos electrónicos se podrán trasladar a copias en soporte papel mediante procedimientos automatizados. En este caso, el documento en soporte papel incorporará un mecanismo que permitirá validar su contenido con la identificación del documento electrónico original. El acceso al documento electrónico original se podrá realizar a través de una dirección electrónica facilitada por la Administración municipal, mediante la utilización de un código seguro de verificación generado electrónicamente.

■ ■ Artículo 41. Archivo electrónico de documentos

1. La Administración municipal adoptará las medidas necesarias para que la mayor parte de los documentos utilizados en las actuaciones administrativas se almacenen en algún soporte electrónico, que permita la conservación de aquéllos. Estos soportes deberán garantizar, además, la integridad, autenticidad, confidencialidad, calidad de los datos contenidos en los mismos, así como la identificación de los usuarios que accedan a los mismos y el control de accesos, en los términos previstos en la legislación sobre protección de datos de carácter personal.
2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de la ciudadanía se conservarán necesariamente en soportes de esa naturaleza, ya sea en el mismo formato a partir del que se generó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para poder reproducirlo. En el caso de que, para una correcta gestión de los intereses en juego, se necesite acceder a dicho documento desde diferentes aplicaciones, la Administración municipal procurará trasladar los datos a otros formatos o soportes que resulten compatibles.
3. Los documentos electrónicos que se reciban y transmitan a través del registro telemático serán archivados y guardados en medios o soportes electrónicos por los responsables de la gestión de los servidores del registro. Sin perjuicio de lo dispuesto en el punto anterior, para su archivo podrá utilizarse el mismo formato o soporte en el que se originó el documento electrónico originario o cualquier otro que asegure la identidad o integridad de la información comprendida en el documento.
4. En cualquier caso, el archivo de documentos electrónicos se realizará de acuerdo con la normativa vigente en materia de gestión documental en lo relativo al cuadro de clasificación, método de descripción y calendario de conservación.

■ ■ Artículo 42. Expediente electrónico

1. Constituye el expediente electrónico aquel conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, independientemente de la clase de información que contengan.
2. Mediante un índice electrónico firmado por la Administración municipal se garantizará el foliado de los expedientes electrónicos, asegurando la integridad del mismo. Cuando un mismo documento haya de formar parte de más de un expediente electrónico, se garantizará la existencia de copias auténticas del mismo en los expedientes electrónicos afectados, en los términos previstos en el artículo 39.1 de la presente Ordenanza.

3. Todos aquellos expedientes electrónicos en los que los ciudadanos posean la condición de interesados, bien sea como titulares, como representantes de aquellos o como titulares de un interés legítimo y directo, estarán disponibles para su consulta por aquéllos en el portal de administración electrónica disponible en la sede electrónica general, previa acreditación de su identidad por los medios previstos en el artículo 17.1 de la presente Ordenanza. Esta consulta, no obstante, podrá limitarse en los casos previstos en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
4. La Administración municipal garantizará el derecho de los interesados a obtener copia del expediente electrónico, en los términos previstos en el artículo 37.8 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, pudiendo sustituirse, a todos los efectos legales, la remisión de expedientes por la puesta a disposición del expediente electrónico. Dicha puesta a disposición del expediente electrónico se producirá, en todo caso, previa identificación y acreditación de la condición de interesado a través de alguno de los medios previstos en el artículo 17.1 de la presente Ordenanza.

■ **TÍTULO IV. De la factura electrónica y el pago electrónico**

■ ■ **Artículo 43. Factura electrónica**

1. La Administración municipal y sus organismos públicos admitirán la presentación, por medios electrónicos, de facturas emitidas por terceros respecto de servicios que les hayan sido prestados, cuando les conste la autenticidad del emisor y del documento y cumpla las demás condiciones establecidas por la normativa correspondiente. Si no constase la veracidad del emisor o del documento, requerirán la misma al emisor para que la acredite por los medios que la Administración estime oportunos.
2. Sin perjuicio de lo previsto en el artículo 28.1 de la presente Ordenanza, la Administración municipal podrá establecer la obligatoriedad de presentación de facturas en formato electrónico, en los casos que oportunamente se determinen en los Manuales de Procedimiento que se aprueben en el Ayuntamiento.
3. La Administración municipal procederá al pago de las cantidades reflejadas empleando preferentemente procedimientos administrativos por medios electrónicos.

■ ■ **Artículo 44. Pago electrónico**

1. La Administración municipal y sus organismos públicos habilitarán sistemas electrónicos de pago que permitan a la ciudadanía el ingreso de tributos, sanciones, multas, recargos u otras cantidades adeudadas a aquéllas, previa liquidación en los casos necesarios.
2. Para el cumplimiento de lo dispuesto en el punto anterior, la Administración municipal podrá valerse de Pasarelas de Pago Electrónico habilitadas por otras Administraciones Públicas, que permitan intercambiar datos *on-line* con determinadas Entidades Financieras de forma segura y confidencial, incorporando con ello el pago *on-line* en cualquier punto de una tramitación telemática.
3. Los sistemas de pago electrónico que se habiliten emitirán el correspondiente impreso justificativo del pago realizado.

■ *Disposiciones adicionales*

■ ■ PRIMERA. Comisión Técnica de Administración Electrónica

Mediante acuerdo de la Junta de Gobierno Local, se constituirá en el Ayuntamiento de Irun una Comisión Técnica de Administración Electrónica, que estará formada por responsables de las Áreas competentes en la materia. Su función será la de promover, planificar y coordinar la implantación efectiva de la Administración Electrónica.

Como apoyo a dicha Comisión Técnica de Administración Electrónica, en el seno de la Administración municipal se podrán crear equipos de trabajo formados por miembros de la primera y determinados referentes de Área de los definidos en el artículo 10 de la presente Ordenanza, cuya función sea la de proponer modificaciones y ampliaciones en el catálogo de trámites y procedimientos electrónicos, dentro de aquellas materias que competencialmente correspondan a dichas Áreas.

■ ■ SEGUNDA. Bilingüismo en la tramitación electrónica

La Administración municipal garantizará el cumplimiento de lo dispuesto en la Ley 10/1982, de 24 de noviembre, Básica de Normalización del Uso del Euskera, en la Ordenanza Municipal sobre Normas para la Normalización del Uso del Euskera en el Ayuntamiento y Municipio de Irun, y en la demás normativa aplicable. En especial, se garantizará que todos los contenidos de las sedes electrónicas municipales se hallen en los dos idiomas oficiales de la Comunidad Autónoma Vasca, garantizando el derecho de la ciudadanía a relacionarse por medios electrónicos en cualquiera de ambas lenguas, de acuerdo a lo previsto en el artículo 36 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

■ *Disposiciones finales*

■ ■ PRIMERA. Implantación de la Administración Electrónica

De acuerdo a lo previsto en la Disposición Final Tercera de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, la Administración municipal garantizará que todos los procedimientos y actuaciones competencia de esta Administración Local que resulten necesarios para la efectiva implantación de la Administración Electrónica, habrán sido efectivamente implantados a 31 de diciembre de 2009, siempre que las disposiciones presupuestarias y el estado de evolución de la tecnología así lo permitan.

■ ■ SEGUNDA. Entrada en vigor

La presente Ordenanza entrará en vigor a los 15 días de su publicación en el Boletín Oficial del Territorio Histórico de Gipuzkoa.

9.3.1. Otras Ordenanzas

Ayuntamiento de Alicante: http://www.alicante.es/documentos/modernizacion/ordenanza_eadmon.pdf

Ayuntamiento de Barcelona: <http://www.bcn.es/orae/cast/>

ANEXO II. *Nuevas Normativas*

10.

10.1. Real Decreto 1671/2009 de 6 de Noviembre

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.

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 determinadas 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 1º. 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 2º. *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 3º. 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 concurren 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 1º. 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 2º. *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 1º. 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 2º. 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» entendiéndose 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», entendiéndose 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 3º. 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 4º. 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 compulsas.**

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 5º. *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 6º. *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.

■ *Disposiciones adicionales*

■ ■ 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».

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ *Disposiciones transitorias*

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ *Disposiciones finales*

■ ■ 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.

■ ■ 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.

■ ■ 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 explicita el cumplimiento de lo dispuesto en el artículo 27.

■ ■ 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.

■ ■ 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.

■ ■ SEXTA. Entrada en vigor

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

Dado en Madrid, el 6 de noviembre de 2009.

10.2. Real Decreto 4/2010 de 8 de Enero. Esquema Nacional de Interoperabilidad

■ *Disposiciones generales*

MINISTERIO DE LA PRESIDENCIA

1331 Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

La 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 redunde 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 1º. 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 I.

■ ■ 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 2º. 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 3º. 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 4º. 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 5º. 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 tendrán 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 6º. 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 7º. 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 8º. *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 9º. 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 atenderán 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 encontrarse 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 unívoca 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 10º. *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 cumplimiento 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.
5. La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

■ **Capítulo 11º. 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 12º. 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.

■ **Disposiciones adicionales**

■ ■ **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 I, 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.
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.

■ ■ 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.

■ ■ 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.

■ ■ 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.

■ *Disposiciones transitorias*

■ ■ 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.

■ ■ 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.

■ *Disposiciones finales*

■ ■ 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.

■ ■ 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.

■ ■ TERCERA. Entrada en vigor

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

Dado en Madrid, el 8 de enero de 2010.

JUAN CARLOS R.

La Vicepresidenta Primera del Gobierno
y Ministra de la Presidencia,
MARÍA TERESA FERNÁNDEZ DE LA VEGA SANZ

■ 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 fijan.
- 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.

10.3. Real Decreto 3/2010 de 8 de Enero. Esquema Nacional de Seguridad

■ *Disposiciones generales*

MINISTERIO DE LA PRESIDENCIA

1330 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.

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 1º. 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 2º. 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 3º. 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. Las 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 información, 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 4º. *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 íntegro 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 5º. 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 auditoría 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.

■ **Capítulo 6º. 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 7º. 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 8º. 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 9º. 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 10º. 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.

■ *Disposiciones adicionales*

■ ■ **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.

■ ■ **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.

■ ■ **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.

■ ■ 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.

■ *Disposiciones finales*

■ ■ 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.

■ ■ 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.

■ ■ TERCERA. Entrada en vigor

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

Dado en Madrid, el 8 de enero de 2010.

JUAN CARLOS R.

La Vicepresidenta Primera del Gobierno
y Ministra de la Presidencia,
MARÍA TERESA FERNÁNDEZ DE LA VEGA SANZ

■ 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:

- 1º. La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
 - 2º. El sufrimiento de un daño menor por los activos de la organización.
 - 3º. El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
 - 4º. Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
 - 5º. 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:

- 1º. La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
 - 2º. El sufrimiento de un daño significativo por los activos de la organización.
 - 3º. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
 - 4º. Causar un perjuicio significativo a algún individuo, de difícil reparación.
 - 5º. 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:

- 1º. La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
- 2º. El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
- 3º. El incumplimiento grave de alguna ley o regulación.
- 4º. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
- 5º. Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

■ ■ 4. Determinación de la categoría de un sistema de información.

1. Se definen tres categorías: BÁSICA, MEDIA y ALTA.
 - a. Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
 - b. Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
 - c. Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.
2. La determinación de la categoría de un sistema sobre la base de lo indicado en el apartado anterior no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

■ ■ 5. Secuencia de actuaciones para determinar la categoría de un sistema:

1. Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3.
2. Determinación de la categoría del sistema, según lo establecido en el apartado 4.

■ Anexo II. *Medidas de seguridad*

■ ■ 1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:
 - a. Las dimensiones de seguridad relevantes en el sistema a proteger.
 - b. La categoría del sistema de información a proteger.
2. Las medidas de seguridad se dividen en tres grupos:
 - a. Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
 - b. Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
 - c. Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

■ ■ 2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

- a. Identificación de los tipos de activos presentes.
 - b. Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
 - c. Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
 - d. Determinación de la categoría del sistema, según lo establecido en el Anexo I.
 - e. Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.
2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.
 3. La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad del sistema.
 4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad, es la que se indica en la tabla siguiente:

Dimensiones				Medidas de Seguridad	
Afectadas	B	M	A		
				org	Marco organizativo
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	Marco operacional
				op.pl	Planificación
categoría	n.a.	+	++	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
AT	aplica	=	=	op.acc.1	Identificación
ICAT	aplica	=	=	op.acc.2	Requisitos de acceso
ICAT	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
ICAT	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
ICAT	aplica	+	++	op.acc.5	Mecanismo de autenticación
ICAT	aplica	+	++	op.acc.6	Acceso local (local logon)
ICAT	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.	aplicada	=	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
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas

Dimensiones				Medidas de Seguridad	
Afectadas	B	M	A		
				mp	Medidas de protección (continuación)
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 del 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
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.

■ ■ 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:

- El uso correcto de equipos, servicios e instalaciones.
- Lo que se considerará uso indebido.
- 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:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- 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:

- Utilización de instalaciones, habituales y alternativas.
- Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces de comunicaciones con otros sistemas.
- Utilización de medios de comunicación, habituales y alternativos.
- Utilización de soportes de información.
- 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	=

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.
- c. Necesidades de comunicación.
- d. Necesidades de personal: cantidad y cualificación profesional.
- e. 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

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	Todas		
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:

- Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
- 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.
- 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	=

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:

- Desarrollo de operación.
- Configuración y mantenimiento del sistema de operación.
- 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 propietario.

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	sí	sí	criptográficos
algo que se es	Biometría	sí	sí	+ doble factor

4.2.6 Acceso local [op.acc.6].

dimensiones	I C A T		
	bajo	medio	alto
nivel	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.

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 propietario; 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	=

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	=

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	=

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

- Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.
- 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.
- Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
- Procedimientos para informar a las partes interesadas, internas y externas.
- 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 el Real Decreto 1720 de 2007, en lo que corresponda.

4.3.8 Registro de la actividad de los usuarios [op.exp.8].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

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

- El registro indicará quién realiza la actividad, cuando la realiza y sobre qué información.
- 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.
- Deben registrarse las actividades realizadas con éxito y los intentos fracasados.
- 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	=

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

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

- Los medios de generación estarán aislados de los medios de explotación.
- Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

- Categoría MEDIA

- Se usarán programas evaluados o dispositivos criptográficos certificados.
- 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	=

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	=

Para la gestión diaria del sistema, se establecerán los siguientes puntos:

- 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]).
- El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.
- 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

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	=

Se realizará un análisis de impacto que permita determinar:

- Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
- 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

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:

- Se identificarán funciones, responsabilidades y actividades a realizar.
- Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.
- Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
- Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- 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

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		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

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

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 atenderá 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	+	=

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	=

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

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	=

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

Se garantizará a 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	+	=

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	+

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.

- Categoría ALTA

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	=	+

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	=	+

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 tránsito
 - 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.

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

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.

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 [mpl.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	=

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	=

- 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	aplica	aplica

Quando 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	+	=

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

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		
	bajo	medio	alto
	no aplica	no aplica	aplica

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	Todas		
categoría	básica	media	alta
	aplica	aplica	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	=

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	aplica	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	aplica	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

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.»

Incidencia del desarrollo reglamentario en la adaptación de las Administraciones Locales a la Ley 11/2007

Anexo a la Guía práctica de la Ley 11/2007,
de Acceso Electrónico de los Ciudadanos
a los Servicios Públicos



Las nuevas normas de desarrollo de la Ley 11/2007, Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), van concretando las acciones a desarrollar dentro del marco de la administración electrónica.

La incidencia de esta nueva normativa en la adaptación de las Entidades Locales a la Ley 11/2007 nos ha llevado, con el impulso de la Comisión de Modernización y Calidad de la FEMP a desarrollar el presente documento con el objetivo de **concretar las directrices y tareas que tienen que definir y llevar a cabo los distintos Ayuntamientos y Diputaciones para poder afrontar el cumplimiento de la Ley 11/2007.**

También hemos querido incluir otras consideraciones no relacionadas directamente con la normativa pero que, como el **liderazgo político**, consideramos esenciales para superar todas las dificultades que encontraremos en nuestro intento de adaptar nuestras organizaciones a la administración electrónica.