

# Comentarios

## SEGURIDAD EN EL COMERCIO ELECTRÓNICO Y FIRMA ELECTRÓNICA

Rubén PÉREZ BAILE  
*Abogado*

---

### *Sumario:*

---

- I. INTRODUCCIÓN.
- II. LA FIRMA ELECTRÓNICA Y EL DOCUMENTO ELECTRÓNICO ANTES DEL REAL DECRETO-LEY 14/1999, DE 17 DE SEPTIEMBRE.
- III. LA FIRMA ELECTRÓNICA EN LA UNIÓN EUROPEA.
- IV. LA FIRMA ELECTRÓNICA EN ESPAÑA.
  - 1. Concepto jurídico de firma electrónica.
  - 2. Prestadores de Servicios de Certificación.
  - 3. Inspección y control de la Autoridad de los Prestadores de Servicios de Certificación.
  - 4. Potestad sancionadora de la Administración en materia de firma electrónica.
- V. EL RÉGIMEN JURÍDICO DE LOS CERTIFICADOS.
  - 1. Requisitos para la existencia de un certificado reconocido.
  - 2. Vigencia de los certificados.
- VI. EFECTOS JURÍDICOS DE LA FIRMA ELECTRÓNICA.

## I. INTRODUCCIÓN.

La evolución de la tecnología desarrollada en tiempos recientes por la industria de la informática está provocando una gran transformación en los sectores económicos: industria, servicios, comercio; y, también, aun cuando se realiza de una forma más pausada, al menos, en España, esta transformación llega ya, incluso, a nivel particular o doméstico.

El uso generalizado de los ordenadores y de Internet (la red de redes, por excelencia) genera un nuevo medio de comunicación, ya que, por lo que se refiere a las empresas, permite que tengan una página web, y, consecuentemente, dar a conocer sus productos y servicios a otras empresas y a los consumidores a nivel global (mundial) a unos costes mínimos, desde el punto de vista económico, si se compara con otras vías o medios de comunicación.

Por tanto, la firma electrónica desde su aprobación por el Real Decreto-Ley 14/1999, de 17 de septiembre, ha venido a convertirse en el mecanismo idóneo para crear documentos electrónicos que deban tener «efectos jurídicos».

No obstante, hay que recordar que la firma electrónica es necesaria para aquellos actos y negocios jurídicos que requieran de firma para su validez, pero no del resto de los actos, donde ésta será un elemento de prueba.

## II. LA FIRMA ELECTRÓNICA Y EL DOCUMENTO ELECTRÓNICO ANTES DEL REAL DECRETO-LEY 14/1999.

El Estado español tuvo una participación activa en el logro de la posición común que facilitó la tramitación de la Directiva Comunitaria (posterior al Real Decreto-Ley 14/1999), al recoger ésta los elementos suficientes para proteger la seguridad y la integración de las comunicaciones telemáticas en las que se emplee la firma electrónica. En este sentido, lejos de lo que pudiera pensarse, España contaba ya, con anterioridad al Real Decreto-Ley, con diversas normas jurídicas de rango legal y normativo en determinados ámbitos, como por ejemplo: la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas (IRPF) por medios telemáticos, dictadas por la Administración Tributaria; la Comisión Nacional del Mercado de Valores (CNMV) que aprobó y puso en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas; o la posibilidad de prestar por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos.

De una forma más detallada vamos a referirnos a una serie de normas jurídicas, sin ánimo de exhaustividad y que son las siguientes:

- a) La Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Ley 30/1992, de 26 de diciembre (LRJAP y PAC) -modificada por la Ley 4/1999, de 10 de enero- en su artículo 45.5 establece que «los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia del documento original siempre que quede garanti-

zada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes».

- b) La Ley del Impuesto sobre el Valor Añadido (IVA), Ley 37/1992, de 28 de diciembre, en su artículo 88.2 establece que «la repercusión del impuesto deberá efectuarse mediante factura o documento análogo, que podrán *emitirse por vía telemática*, en las condiciones y con los requisitos que se determinen reglamentariamente».

Esta posibilidad fue desarrollada por la Orden de 22 de marzo de 1996, por la que se dictan las normas de aplicación del sistema de facturación telemática previsto en el artículo 88 de la Ley 37/1992, de 28 de diciembre, del IVA.

- c) La Ley del Mercado de Valores, Ley 24/1988, de 24 de julio, regula las operaciones de Bolsa que se llevan a cabo mediante el Sistema de Interconexión Bursátil, integrado, como señala la propia exposición de motivos de la Ley, mediante una red informática; y el Acuerdo de 11 de marzo de 1998 de la CNMV sobre implantación de CIFRADOC/CNMV -sistema de intercambio de información a través de líneas telemáticas-.
- d) A través de <http://aeat.es> se tiene acceso a una serie de órdenes que regulan la declaración del IRPF para grandes empresas, PYMES y contribuyentes. Además, el procedimiento para la obtención e instalación de certificado con firma electrónica para hacer la declaración del IRPF puede obtenerse en <http://aeat.es/certfnmt.html>.
- e) La Orden de 19 de julio de 1999, por la que se aprueba el Registro de Compraventa de Bienes Muebles a Plazos, en su disposición adicional sexta, autoriza a la Dirección General de Registros y del Notariado para aprobar modelos en soporte informático o con firma electrónica, siempre que se garantice la identidad indubitada de los contratantes y la integridad e inalterabilidad del documento.
- f) La Ley de Medidas Fiscales, Administrativas y del Orden Social, Ley 66/1997, de 30 de diciembre, en el artículo 81 anuncia la posibilidad de prestar por la Fábrica Nacional de Moneda y Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos. La Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda actuará en colaboración con Correos y Telegráfos.
- g) En el ámbito procesal, y a los efectos de determinar la validez de los documentos electrónicos como medios de prueba, la Ley Orgánica del Poder Judicial, Ley 6/1985, de 1 de julio, en su artículo 230 establece que «Los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos para el desarrollo de su actividad y ejercicio de sus funciones ...

Los documentos emitidos (señala su párrafo segundo) gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales».

### III. LA FIRMA ELECTRÓNICA EN LA UNIÓN EUROPEA.

El 16 de abril de 1997, la Comisión presentó al Parlamento Europeo, al Consejo y al Comité Económico y Social y al Comité de las Regiones la comunicación «Iniciativa europea de comercio electrónico».

El 8 de octubre de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación «El Fomento de la Seguridad y la confianza en la comunicación electrónica: hacia un marco europeo para la firma digital y cifrado».

Dados estos antecedentes, con fecha de 1 de diciembre de 1997, el Consejo invitó a la Comisión a que presentara lo antes posible una propuesta de directiva del Parlamento Europeo y del Consejo sobre la firma digital. Esto se produjo con la Posición Común (CE) número 1999/C 243/02, de 28 de junio, del Consejo con vistas a la adopción de la Directiva 1999/.../CE del Parlamento Europeo y del Consejo ... por la que se establece un marco comunitario para la firma electrónica, y la Decisión del Parlamento Europeo de 27 de octubre de 1999, lo cual dio lugar a la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica (DOCE L 13, de 19 de enero de 2000).

La Directiva entró en vigor el día 19 de enero del año 2000 y los Estados miembros deben poner en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la Directiva, a no más tardar el 19 de julio de 2001 (arts. 13 y 14).

En su considerando (4) la Directiva comunitaria insiste en que la comunicación y el comercio electrónico requieren firmas electrónicas y servicios conexos de autenticación de datos, y la heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico. Por otro lado, un marco claro comunitario sobre las condiciones aplicables a la firma electrónica aumenta la confianza en las nuevas tecnologías y la aceptación general de las mismas; consecuentemente, los Estados miembros no deben obstaculizar en este ámbito la libre circulación de bienes y servicios en el mercado interior.

Dado que el mercado interior garantiza la libre circulación de personas, es cada vez más frecuente que los ciudadanos y residentes de la Unión Europea tengan que tratar con autoridades de Estados miembros distintos de aquel en el que residen. Por ello, la disponibilidad de la comunicación electrónica es de gran utilidad.

En este sentido, el mercado interior permite a los proveedores de servicios de certificación llevar a cabo sus actividades transfronterizas para acrecentar su competitividad y ofrecer a los consumidores y a las empresas nuevas posibilidades de intercambiar información y comerciar electrónicamente de una forma segura, con independencia de las fronteras.

La fórmula para estimular la prestación de servicios de certificación en toda la Comunidad a través de redes abiertas se consigue porque los proveedores de servicios de certificación deben tener libertad para prestar sus servicios sin autorización previa; si bien se pueden introducir limitaciones nacionales a la prestación de tales servicios, siempre que sean justificadas y proporcionadas y no impidan el régimen de libre competencia dentro de la Unión Europea.

A continuación, reseñamos brevemente el contenido fundamental de la Directiva:

La Directiva consta de 15 artículos y tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. La presente Directiva crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior (art. 1.º).

Además, se comprometen los Estados miembros a no condicionar la prestación de servicios de certificación a la obtención de autorización previa, sin perjuicio de que los Estados miembros pue-

dan establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación (art. 3.º).

Por lo que respecta a los efectos jurídicos de la firma electrónica, la Directiva determina que los Estados miembros deben procurar que la firma electrónica «avanzada» basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma: satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación a los datos en papel; y sea admisible como prueba en procedimientos judiciales (art. 5.º).

Se debe garantizar que el proveedor de servicios de certificación que expida al público un certificado presentado como certificado reconocido o que garantice al público tal certificado, será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en el certificado por lo que respecta a veracidad y garantía, salvo que se demuestre que el proveedor de servicios de certificación no ha actuado con negligencia (art. 6.º).

Además, se debe velar por que los certificados expedidos al público como certificados reconocidos por un proveedor de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si cumple una serie de requisitos fijados en la actual Directiva, como son el haber sido acreditado en el marco de un sistema voluntario de acreditación, avale el certificado y se reconozca un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones (art. 7.º).

La Directiva obliga a que los Estados miembros velen por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1975, relativa a la protección de datos personales y a la libre circulación de los mismos (art. 8.º).

#### IV. LA FIRMA ELECTRÓNICA EN ESPAÑA.

##### 1. Concepto jurídico de firma electrónica.

El concepto jurídico de firma electrónica es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados fundamentalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

Así, por ejemplo, la firma del propio sujeto escaneada e incorporada a un documento electrónico es una firma electrónica.

Sin embargo, la *firma electrónica avanzada* basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma debe satisfacer el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos de papel, y además, debe ser admisible como prueba en procedimientos judiciales.

Por tanto, debemos distinguir entre firma electrónica y firma electrónica avanzada, porque son precisamente las presunciones legales, en la firma electrónica avanzada, las que permitirán que este instrumento técnico se generalice y sea considerado en la vida cotidiana como un equivalente a la firma manuscrita con su mismo valor y eficacia jurídica.

El artículo 2.º del Real Decreto-Ley 14/1999 distingue entre *firma electrónica*, que «es el conjunto de datos, en forma electrónica ... utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge» y *firma electrónica avanzada* que «es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos».

En este sentido, el artículo 3.º del Real Decreto-Ley 14/1999 considera que la *firma electrónica* tendrá el efecto que en cada caso concreto pueda reconocérsele por un Juez, dentro de su libre apreciación, con lo que su eficacia jurídica, a priori, queda limitada. Sin embargo, y he aquí el hecho diferencial y el aporte legislativo, la *firma electrónica avanzada* queda equiparada por la ley, a la firma manuscrita siempre que reúna las condiciones y requisitos técnicos como son que se base, primero, en un *certificado reconocido* y, segundo, en un *dispositivo seguro de creación de firma*, reconociéndose su admisión como prueba en juicio.

Por último, con objeto de comprender el planteamiento técnico de este sistema indicar que el mecanismo de la firma electrónica se basa en una firma digital, firma digital que consiste en una combinación de números y letras que forman una cadena lo suficientemente larga como para garantizar que es imposible la existencia de una cadena igual para identificar a otras personas, a la cual se añaden dos elementos más constituidos por dos pares de claves: una clave pública y una clave privada. La finalidad de estas claves es encriptar el documento electrónico al que se añade la firma como el documento en el que se contiene la firma y que va unido al documento gracias a una función del correo electrónico.

Estas claves están íntimamente ligadas de modo que a una clave pública determinada sólo puede corresponderle una clave privada.

La clave privada es aquella que sólo es conocida por la persona firmante, mientras que la clave pública es conocida por todos. Así, si firmamos determinado documento con nuestra clave privada cualquiera podrá reconocerlo como nuestro si utilizando nuestra clave pública un programa informático específico así lo verifica.

Concluyendo, cuando la firma identifica a su autor de una forma totalmente fiable y permite detectar cualquier alteración del documento no autorizada merced a que los mecanismos utilizados en la creación de la firma son seguros, por cumplir ciertas exigencias técnicas, y por que el prestador de servicios de certificación que ha intervenido está «acreditado», entonces se habla de firma electrónica avanzada; la cual gozará de una mayor eficacia jurídica que una simple firma electrónica.

## 2. Prestadores de servicios de certificación.

Antes de comenzar a ver los distintos apartados de este punto debemos definir la figura del prestador de servicios de certificación.

En este sentido, prestador de servicios de certificación «es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica».

Además, hay que tener en cuenta que la norma jurídica que desarrolla la prestación de servicios de certificación es la Orden de 21 de febrero de 2000, del Ministerio de Fomento, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

La Secretaría General de Comunicaciones del Ministerio de Fomento es el órgano competente para, salvaguardando la seguridad en las comunicaciones, acreditar a los prestadores de servicios de certificación y certificar los productos de firma electrónica, que cumplan las siguientes condiciones:

- Que estén destinados a conectarse directa o indirectamente a los puntos de terminación de una red pública de telecomunicaciones, con el objeto de enviar, procesar o recibir señales.
- Que estén destinados a garantizar la seguridad de cualquier tipo de información que se transmita por vía electrónica por redes de telecomunicaciones.

Sin embargo, cabe recordar que el propio Reglamento incide en la cuestión de que la regulación del sistema de acreditación y de certificación de los productos de firma electrónica se refiere únicamente a aquellos productos de firma electrónica respecto de los que es competente la Secretaría General de Comunicaciones del Ministerio de Fomento. Y que el sometimiento a los sistemas de acreditación y de certificación regulados en el Reglamento es voluntario.

No obstante, no cabe duda de que el Reglamento confiere un alto grado de seguridad, calidad y confianza en la prestación de servicios de certificación que se traslada a una mayor protección de los derechos de los usuarios, al verse protegidos por los sistemas de acreditación de prestadores de servicios de certificación y de certificación, pues para obtener la acreditación es necesario demostrar el cumplimiento de los requisitos técnicos que reglamentariamente se fijan.

La Orden de 21 de febrero de 2000 regula el sistema de acreditación y de certificación, las entidades de evaluación, los órganos de acreditación y certificación y coordinación con otros sistemas de certificación, la acreditación de prestadores de servicios de certificación y la certificación de dispositivos seguros de creación de firma y dispositivos de verificación de firma electrónica avanzada.

En este sentido, la Secretaría General de Comunicaciones certifica como dispositivos seguros de creación de firma, los dispositivos que garantizan:

- Que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente (dice RDL 14/1999) su secreto.
- Que existe seguridad razonable de que estos datos no pueden ser derivados de los de verificación de firma o de la propia firma.
- Que la firma no pueda ser falsificada con la tecnología existente en cada momento.
- Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros, y
- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

### *2.1. Registro de Prestadores de Servicios de Certificación.*

Es el artículo 7.º del Real Decreto-Ley 14/1999 donde se regula el Registro de Prestadores de Servicios de Certificación. En este Registro (se crea en el Ministerio de Justicia) deben solicitar su inscripción todos los prestadores de servicios de certificación.

El Registro, que será público, deberá mantener permanentemente actualizada y a disposición de cualquier persona una relación de los inscritos.

Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral.

No obstante, esta información podrá sujetarse al pago de una tasa, cuyos elementos esenciales deben determinarse por Ley.

### *2.2. Obligaciones de los prestadores de servicios de certificación.*

Las obligaciones que vienen recogidas en el artículo 11 del Real Decreto-Ley 14/1999 son las siguientes:

- Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de dicha obligación, los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.
- Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.
- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.
- Mantener un registro de certificados, en el que guardará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o pérdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará en disposición de las personas que lo soliciten, cuando así lo autorice el signatario.
- En el caso de cesar en su actividad, los prestadores de servicios de certificación, deberán comunicarlo con una antelación mínima de dos meses al cese efectivo, a los titulares de los certificados por él expedidos y transferir, con su consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto.  
Y, si el prestador de servicios estuviera inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar, a éste, con la antelación anterior referida, el cese de su actividad, y el destino que vaya a dar a los certificados especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto.
- Y, por último, solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

### *2.3. Obligaciones de los Prestadores de Servicios de Certificación que expidan certificados reconocidos.*

Cuando el prestador de servicios de certificación expide certificados reconocidos, además de cumplir las obligaciones enumeradas en el punto 2.1 y 2.2 de este estudio, deben cumplir las siguientes:

- Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.
- Demostrar la fiabilidad necesaria de sus servicios.
- Garantizar la rapidez y la seguridad en el servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de Certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.
- Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.
- Disponer de los suficientes recursos económicos al objeto de poder afrontar un posible riesgo de responsabilidad por daños y perjuicios. La garantía (frente a usuarios de sus servicios y terceros afectados por éstos) debe cubrir, al menos, inicialmente, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación (el gobierno puede mediante Real Decreto reducir el porcentaje hasta el 2 por 100).  
Sin embargo, en caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 6.010.121 euros (el gobierno puede mediante Real Decreto modificar este importe).
- Conservar registrada toda la información y documentación relativa a un certificado reconocido durante 15 años. Esta actividad de registro podrá realizarse por medios electrónicos.
- Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quién lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.
- Utilizar sistemas fiables para almacenar certificados, de modo tal que:
  1. Sólo personas autorizadas puedan consultarnos, si éstos únicamente están disponibles para verificación de firmas electrónicas.
  2. Únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.
  3. Pueda comprobarse la autenticidad de la información.
  4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.
- Y, por último, informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando el Real Decreto-Ley 14/1999 y sus disposiciones de desarrollo, en el ejercicio de su actividad.

### 3. Inspección y control de la actividad de los prestadores de servicios de certificación.

El Ministerio de Fomento, controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en el Real Decreto-Ley 14/1999 y en sus disposiciones de desarrollo. Asimismo, vigilará el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones establecidas en el artículo 11 del Real Decreto-Ley 14/1999 (las obligaciones se han recogido en el apdo. 4.2.2 de este estudio).

En el ejercicio de su actividad de control, la Secretaría General de Comunicaciones actuará de oficio, mediante petición razonada del Ministerio de Justicia o de otros órganos administrativos o a instancia de persona interesada. Los funcionarios de la Secretaría General de Comunicaciones adscritos a la Inspección de las Telecomunicaciones, a efectos de cumplir las tareas de control, tendrán la consideración de autoridad pública.

Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención del tratamiento de datos, de lo dispuesto en el artículo 11 c) del Real Decreto-Ley 14/1999 (ejemplo, no almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Ésta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador.

Señalar, que los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría General de Comunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, referida siempre a datos que conciernen al prestador de servicios.

Y, por último, señalar, que la Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan el Real Decreto-Ley 14/1999 y las disposiciones de desarrollo.

### 4. Potestad sancionadora de la Administración en materia de firma electrónica.

#### 4.1. Infracciones.

Las infracciones de las normas reguladoras de la firma electrónica y de los servicios de certificación se clasifican en muy graves, graves y leves. Se encuentran tipificadas en el artículo 25 del Real Decreto-Ley 14/1999.

- Son infracciones muy graves:
  - El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h), es decir, las siguientes: comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin pro-

pio de éstos, utilizando cualquiera de los medios admitidos en derecho; poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica; informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial; mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o pérdida de vigencia de sus efectos; en el caso de cesar en su actividad los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el apartado 1 del artículo 13 (dos meses), a los titulares de los certificados por ellos emitidos y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

- El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones impuestas en las letras c) a la j) del artículo 12, siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación, es decir, las siguientes: garantizar la rapidez y la seguridad en la prestación del servicio; emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados; utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte; tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación; disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en el Real Decreto-Ley 14/1999; conservar registrada toda la información y documentación relativa a un certificado reconocido durante 15 años; antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado; y, utilizar sistemas fiables para almacenar certificados.
  - El incumplimiento grave y reiterado por los prestadores de servicios de certificación de las resoluciones dictadas por la Secretaría General de Comunicaciones, para asegurar el respeto al Real Decreto-Ley 14/1999.
- Son infracciones graves:
    - El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones impuestas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h) siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.
    - El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones previstas en las letras a), b), y k) del artículo 12, es decir, el incumplimiento de las siguientes obligaciones: indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado; demostrar la fiabilidad necesaria de sus servicios; e informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando el Real Decreto-Ley 14/1999 y sus disposiciones de desarrollo, en el ejercicio de su actividad.

- El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones contempladas en las letras c) a la j) del artículo 12, siempre y cuando no concurren las circunstancias previstas en el apartado anterior [obligaciones previstas en las letras a), b) y k) del art. 12].  
La falta de comunicación por el prestador de servicios de certificación al Ministerio de Justicia, en los plazos previstos en el artículo 13, es decir, en el plazo mínimo de dos meses, del cese de su actividad o de la iniciación, respecto de él, de un procedimiento de suspensión de pagos o de quiebra.
  - La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo, con arreglo al Real Decreto-Ley 14/1999.
  - El incumplimiento de las resoluciones dictadas por la Secretaría General de Comunicaciones para asegurar que el prestador de servicios de certificación se ajustan al Real Decreto-Ley 14/1999, cuando no deba considerarse como infracción muy grave.
- Son infracciones leves:
- El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11 (reseñadas anteriormente en las infracciones muy graves) a excepción de la c), es decir, la obligación de no almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite, ya que esta última podría considerarse según las circunstancias como una infracción grave.
  - La expedición de certificados reconocidos que incumplan alguno de los requisitos establecidos en el artículo 8.º del Real Decreto-Ley 14/1999. Es decir, el incumplimiento de alguno de estos contenidos: la indicación de que se expiden como tales certificados reconocidos; el código identificativo único del certificado; la identificación del prestador de servicios de certificación que expide el certificado; la firma electrónica avanzada del prestador de servicios de certificación que expide el certificado; la identificación del signatario; en caso de representación el documento que acredite tal facultad al signatario; los datos de verificación de firma que corresponden a los datos de creación; el comienzo y el fin del período de validez del certificado; los límites de uso del certificado, si se prevén; y, los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.
  - No facilitar los datos requeridos, en el ámbito de sus respectivas funciones, por el Ministerio de Justicia o la Secretaría General de Comunicaciones para comprobar el cumplimiento del Real Decreto-Ley 14/1999 por los prestadores de servicios de certificación.
  - Cualquier otro incumplimiento de las obligaciones impuestas a los prestadores de servicios de certificación por el Real Decreto-Ley 14/1999, salvo el ya mencionado del artículo 11 c), por cuanto pudiera ser considerado bien como infracción muy grave o grave.

#### 4.2. Sanciones.

Las sanciones por la comisión de infracciones relatadas en el punto anterior se recoge en el artículo 26 del Real Decreto-Ley 14/1999.

Por tanto, por la comisión de *infracciones muy graves*, dice el artículo, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quintuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: el 1 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 5 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 601.012,10 euros.

La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de las circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años. Cuando la resolución de imposición de esta sanción sea firme, será comunicada en el Registro de Prestadores de Servicios de Certificación para que cancele la inscripción del prestador de servicios sancionado.

Por la comisión de *infracciones graves*, se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: el 0,5 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 2 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 300.506,04 euros.

Por la comisión de *infracciones leves* se impondrá al infractor una multa por importe de hasta 12.020,23 euros.

Además, de todo lo anterior, la propia norma regula la posibilidad de que las infracciones muy graves y graves llevaran aparejada la publicación de la resolución sancionadora en el «Boletín Oficial del Estado» y en dos periódicos de difusión nacional una vez, eso sí, que tuviera el carácter de firme.

También, aclara, que las infracciones graves y muy graves se anotarán en el Registro de Prestadores de Servicios de Certificación. Las notas relativas a las sanciones se cancelarán una vez transcurridos los plazos de prescripción de las sanciones administrativas previstas en la propia LRJAP y PAC (Ley 30/1992, en la redacción dada por la Ley 4/1999).

#### 4.3. Procedimiento sancionador.

Determina el artículo 28 del Real Decreto-Ley 14/1999 que el ejercicio de la potestad sancionadora corresponde a la Secretaría General de Comunicaciones del Ministerio de Fomento. Como todo acto administrativo, el procedimiento aplicable es el procedimiento administrativo común regulado en la LRJAP y PAC, Ley 30/1992, que fue modificado por la Ley 4/1999, siendo su actual redacción la vigente y válida jurídicamente.

Cabe resaltar, por último, la posibilidad de dictar medidas cautelares en los procedimientos por infracciones muy graves y graves, según lo determinado en la Ley 30/1992, de 26 de noviembre, LRJAP y PAC, modificada, como anteriormente se ha señalado, por la Ley 4/1999, de 10 de enero.

La medida cautelar podrá consistir en la orden de cese temporal de la actividad del prestador de servicios de certificación, en la suspensión de la vigencia de los certificados por él expedidos o en la adopción de otras cautelas que se estimen precisas.

## V. EL RÉGIMEN JURÍDICO DE LOS CERTIFICADOS.

Ya vimos que el Real Decreto-Ley 14/1999 definía certificado como aquella certificación electrónica que vincula unos datos de verificación de firma (son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica) a un signatario y confirma su identidad.

Además, definía, asimismo, el certificado reconocido, como aquel certificado que contiene la información descrita en el artículo 8.º y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12. En consecuencia, aunque ya ha quedado matizado a lo largo del presente estudio, vamos a enumerar los requisitos para la existencia de un certificado reconocido y la vigencia de los certificados.

### 1. Requisitos para la existencia de un certificado reconocido.

Como ya hemos señalado, dichos requisitos se recogen en el artículo 8.º del Real Decreto-Ley 14/1999. Son los siguientes, y tendrán el siguiente contenido:

- La indicación de que se expiden como tales.
- El código de identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.
- La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.
- En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.
- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.
- El comienzo y el fin del período de validez del certificado.
- Los límites de uso del certificado, si se prevén.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

En cualquier caso, si además de las especificaciones vistas, se quiere consignar en el certificado otra información relativa al signatario, requerirá el consentimiento expreso de éste.

## 2. Vigencia de los certificados.

El artículo 9.º del Real Decreto-Ley 14/1999, regula las circunstancias, en las cuales el certificado de firma electrónica queda sin efecto. En este sentido, pues, los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:

- Expiración del período de validez del certificado (si el certificado es un certificado reconocido este plazo no podrá ser superior a cuatro años, contados desde la fecha de expedición).
- Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.
- Pérdida o inutilización por daños del soporte del certificado.
- Utilización indebida por un tercero.
- Resolución judicial o administrativa que lo ordene.
- Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en un Registro de Certificados, en el que deberá quedar constancia de los emitidos y figurarán las circunstancias que afectan a la suspensión o pérdida de vigencia de sus efectos. A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.

Asimismo, el prestador de servicios de certificación responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación. Corresponderá al prestador de servicios de certificación la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

Señalar que la responsabilidad de los prestadores de servicios de certificación se encuentra regulada en el artículo 14 del Real Decreto-Ley 14/1999.

Por último, indicar que el prestador de servicios de certificación podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa.

## VI. EFECTOS JURÍDICOS DE LA FIRMA ELECTRÓNICA.

El Real Decreto-Ley 14/1999, definía la *firma electrónica* como el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Mas allá, definía la *firma electrónica avanzada* como aquella que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Vistas, ambas definiciones, nos referiremos a continuación a los efectos jurídicos de la firma electrónica. Dichos efectos, hay que recordar, vienen regulados en el artículo 3.º del Real Decreto-Ley 14/1999.

El artículo 3.º 1 indica que la firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21.

Esto quiere decir, que es necesaria la evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica. Serán las entidades de evaluación las que aplicarán las normas técnicas respecto de los productos de firma electrónica. El desarrollo de estas cuestiones (arts. 21 y 22 RDL 14/1999), se realizó mediante la Orden de 21 de febrero de 2000, del Ministerio de Fomento, por el que se aprueba el Reglamento de acreditación de prestadores de servicios de certificados y de certificación de determinados productos de firma electrónica.

Sin embargo, el artículo 3.º 2 Real Decreto-Ley 14/1999 nos dice que a la firma electrónica que no reúna todos los requisitos previstos en el apartado 3.1, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

En resumen, el Real Decreto-Ley 14/1999, distingue:

- a) Firma electrónica avanzada, y
- b) Firma electrónica.

Consecuentemente, la *firma electrónica avanzada* (basada en un certificado reconocido y dispositivo seguro de creación de firma):

- Será admisible como prueba en juicio, valorándose según los criterios de apreciación establecidos en las normas procesales. Es decir, sea admisible como prueba en procedimientos judiciales, y
- Su valor jurídico es el mismo que la firma manuscrita. Es decir, satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel.

Sin embargo, la *firma electrónica* (no es avanzada y no está basada en un certificado reconocido):

- No se le niegan los efectos jurídicos, ni se le excluye como prueba en juicio, pero queda por definir cuál será la norma que especifique su eficacia. Es decir, no se le niega la eficacia jurídica, ni la admisibilidad como prueba en procedimiento judicial, a la firma electrónica por el mero hecho de que: ésta se presente en forma electrónica, o no se base en un certificado reconocido, o no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o no esté creada por un dispositivo seguro de creación de firma.