

TEMA 22: LA FIRMA ELECTRÓNICA.

Autora: Olivia Suárez Quintana.
Licenciada en Derecho por la Universidad de Las Palmas de Gran Canaria.
Funcionaria de la Comunidad Autónoma de Canarias.

MARCO NORMATIVO.

Legislación Española

- **Ley 59/2003, de 19 de diciembre, de firma electrónica.**
- Real Decreto-Ley 14/1999, de 17 de septiembre por el cual se regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.
- Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
- Proyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de Firma Electrónica.
- 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.
- **Ley 30/1992, de 26 de Noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.**
- **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.**
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial [art. 230].
- ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.
- ORDEN ECO/2579/2003, de 15 de septiembre, por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Ministerio de Economía y sus Organismos adscritos.
- ORDEN EHA/3256/2004, de 30 de septiembre, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 35.4 de la Ley General Tributaria.

Legislación Comunitaria.

- 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.
- DECISIÓN DE LA COMISIÓN de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE de Parlamento Europeo y del Consejo.

Legislación del Gobierno Autónomo Canario.

- Decreto 205/2001, de 3 de diciembre, por el que se regula el empleo de la firma electrónica en los procedimientos administrativos de la Administración Pública de la Comunidad Autónoma de Canarias.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, modificada por la Ley 4/1999, de 13 de enero, introduce la informatización como un elemento de necesaria incorporación al procedimiento administrativo, estableciendo en su artículo 45 un mandato de carácter programático a las Administraciones Públicas para que se impulse la utilización y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos en el ejercicio de sus competencias.

Así mismo, reconoce a los ciudadanos la facultad de relacionarse con las diferentes Administraciones y el ejercicio de sus derechos ante ellas utilizando las técnicas o medios electrónicos, informáticos o telemáticos, otorgándoles a los documentos y copias así realizados validez y eficacia jurídica siempre que se cumplan los requisitos previstos en la Ley y se garantice la autenticidad, integridad, conservación y, en su caso, la recepción por el interesado, así como el resto de garantías exigidas por la Ley o por otras normas que resulten de aplicación.

Para garantizar el cumplimiento de los requisitos antes señalados, se dicta el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, en el que se establecen los requisitos técnicos que deben cumplir los instrumentos tecnológicos a fin de acreditar la identificación del firmante y lograr la autenticidad e integridad de los documentos electrónicos y con ello eficacia jurídica en las relaciones administrativas a través de medios electrónicos.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, se promulga para reforzar el marco jurídico existente incorporando a su texto algunas novedades respecto del Real Decreto-ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

Así, se revisa la terminología, se modifica la sistemática y se simplifica el texto facilitando su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa.

Una de las **novedades** que la Ley ofrece respecto del **Real Decreto-ley 14/1999**, es la denominación como **firma electrónica reconocida** que se equipara funcionalmente a la **firma manuscrita**. Se trata simplemente de la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la **Directiva 1999/93/CE** como el propio **Real Decreto-ley 14/1999** venían exigiendo. Con ello se aclara que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un **certificado reconocido** y haya sido creada por un **dispositivo seguro de creación**.

Asimismo, es de destacar de manera particular, la **eliminación del registro de prestadores de servicios de certificación**, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

Por otra parte, la Ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva. Así, se **favorece la autorregulación de la industria**, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación. El nuevo régimen nace desde el convencimiento de que los **sellos de calidad** son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público. Si bien se recogen fielmente en la Ley los conceptos de *acreditación* de prestadores de servicios de certificación y de *conformidad* de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la **Ley 21/1992, de 16 de julio, de Industria**.

Otra modificación relevante es que la Ley clarifica la **obligación de constitución de una garantía económica** por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Por otra parte, dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la Ley **refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología**, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas

para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

También ha de destacarse la regulación que la Ley contiene respecto del **documento nacional de identidad electrónico**, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La Ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus **dos notas** más características **-acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos-** remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

Asimismo, otra novedad es el establecimiento en la Ley del régimen aplicable a la **actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático**. Se va así más allá del **Real Decreto-ley de 1999**, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.

En todo caso, los **certificados electrónicos de personas jurídicas** no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la Ley exige, por un lado, una **especial legitimación** para que las personas físicas soliciten la expedición de certificados; por otro lado, **obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados**, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario **Código de Comercio** regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Adicionalmente, se añade un régimen especial para **la expedición de certificados electrónicos a entidades sin personalidad jurídica** a las que se refiere el **artículo 33 de la**

Ley General Tributaria, a los **solos efectos de su utilización en el ámbito tributario**, en los términos que establezca el Ministerio de Hacienda.

Por otra parte, siguiendo la pauta marcada por la **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico**, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Además, debe resaltarse que otro aspecto novedoso de la Ley es el acogimiento explícito que se efectúa de las **relaciones de representación** que pueden subyacer en el empleo de la firma electrónica. No cabe duda que el instituto de la representación está ampliamente generalizado en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica. Para ello, se establece como novedad que en la expedición de certificados reconocidos que admitan entre sus atributos relaciones de representación, ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante. Asimismo, se prevén mecanismos para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.

Por último, debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer **mecanismos de coordinación** con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante **conexiones telemáticas**, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos. Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores

Por su parte, el **Gobierno de Canarias** es consciente de la necesidad de promover el uso de las tecnologías de la información y la comunicación como medio para conseguir un mayor acercamiento a la sociedad del conocimiento. Para ello ha puesto en marcha el **Plan Canari@s Digital**. Entre sus objetivos se encuentra el conseguir una mejora de los servicios públicos que presta la Administración a los ciudadanos simplificando el acceso a los mismos. Por ello es preciso poner en marcha en el conjunto de los organismos públicos la posibilidad de interactuar directamente con la Administración a través de medios telemáticos lo que requiere el uso de técnicas de identificación inequívocas como es la firma electrónica.

De acuerdo con lo expuesto, resulta ineludible seguir avanzando en el campo jurídico de la regulación de la utilización de las técnicas electrónicas, informáticas y telemáticas en la Administración Pública de la Comunidad Autónoma de Canarias al ser determinantes para la tramitación utilizando estos medios con total garantía para la Administración y el ciudadano.

El artículo 32.6 de la Ley Orgánica 10/1982, de 10 de agosto, de Estatuto de Autonomía de Canarias, según reforma operada por la Ley Orgánica 4/1996, de 30 de diciembre, atribuye a la Comunidad Autónoma de Canarias competencias de desarrollo legislativo y la ejecución en materia de régimen jurídico de la Administración Pública de la Comunidad Autónoma y de los entes públicos dependientes.

El Decreto 205/2001, de 3 de diciembre regula la **utilización de firma electrónica en los procedimientos administrativos** tramitados por los distintos Departamentos de la Administración Pública de la Comunidad Autónoma de Canarias, sus Organismos Autónomos y Entidades de Derecho Público vinculadas a la misma.

A efectos de dar **eficacia jurídica y seguridad a las relaciones administrativas** en las que se utilice la firma electrónica, la Consejería competente en materia de tecnologías de la información, mediante los procedimientos legalmente establecidos, seleccionará a aquellas entidades prestadoras de servicios de certificación, que provean de firma electrónica avanzada que esté basada en un certificado reconocido y se produzca por un dispositivo seguro de creación de firma.

La Administración Pública de la Comunidad Autónoma de Canarias asumirá las **funciones de intermediación** entre los prestadores de servicios de certificación y los interesados en las tareas de comprobación de la identidad y cualesquiera otras circunstancias personales que deban figurar en los certificados electrónicos que se emitan.

Corresponde al Departamento competente en materia de tecnologías de la información el **establecimiento y desarrollo de las normas y características que deban cumplir los elementos técnicos** cuya finalidad es posibilitar y garantizar la seguridad en la tramitación mediante firma electrónica. Con este fin, desarrollará el archivo de documentos electrónicos originales, el directorio electrónico de cargos y funciones, la base de datos de terceros que se relacionen mediante firma electrónica con la Administración y cualesquiera otros elementos técnicos precisos para la tramitación electrónica.

Para cada procedimiento que se tramite mediante firma electrónica se publicarán por el Departamento u organismo correspondiente, conjuntamente con la Consejería competente en materia de tecnologías de la información, los **requerimientos técnicos necesarios** para acceder a la tramitación administrativa a través de dichas técnicas.

Asimismo, corresponde al titular del Departamento competente en materia de tecnologías de la información la suscripción de los acuerdos y convenios que procedan con las Entidades locales e Instituciones públicas de la Comunidad Autónoma de Canarias para el establecimiento de procedimientos comunes de certificación electrónica.

A efectos de la **acreditación de la presentación**, la documentación tramitada por vía electrónica, con los requisitos que se establezcan para cada procedimiento, tendrá la misma validez y eficacia que la presentada en soporte papel, debiendo estarse a la legislación de procedimiento común en cuanto a la iniciación del procedimiento.

Asimismo, las fechas de transmisión y recepción acreditadas en las comunicaciones y notificaciones efectuadas por esta vía, serán válidas a efectos del cómputo de plazos y términos.

Por los órganos competentes, se dictarán las normas y adoptarán los procedimientos técnicos que sean precisos para hacer efectivo el servicio.

2. DISPOSICIONES GENERALES SOBRE LA FIRMA ELECTRÓNICA.

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la **confianza de la ciudadanía en las comunicaciones telemáticas**. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de **conferir seguridad a las comunicaciones** por Internet surge, entre otros, la firma electrónica. **La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.**

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados **prestadores de servicios de certificación**. Para ello **expiden certificados electrónicos**, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La Ley obliga a los prestadores de servicios de certificación a **efectuar una tutela y gestión permanente de los certificados electrónicos que expiden**. Los detalles de esta gestión deben recogerse en la llamada **declaración de prácticas de certificación**, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un **servicio de consulta** sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Es una cadena de caracteres, generada mediante un algoritmo matemático, que se obtiene utilizando como variables la **clave privada** y la **huella digital** del texto a firmar de forma que permite **asegurar la identidad del firmante y la integridad del mensaje**.

Dentro del término de firma electrónica caben destacar las siguientes **concepciones**:

La **firma electrónica avanzada**: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

La **firma electrónica reconocida**: se considera la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

¿Qué garantía ofrece la firma electrónica?

- **Autenticación**: Identifica al usuario que ha enviado el mensaje.
- **Integridad**: Garantiza que no se ha alterado el mensaje.
- **No repudio**: Nadie excepto el emisor podría haber firmado el documento.

Se considera **documento electrónico** el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.

El documento electrónico será soporte de:

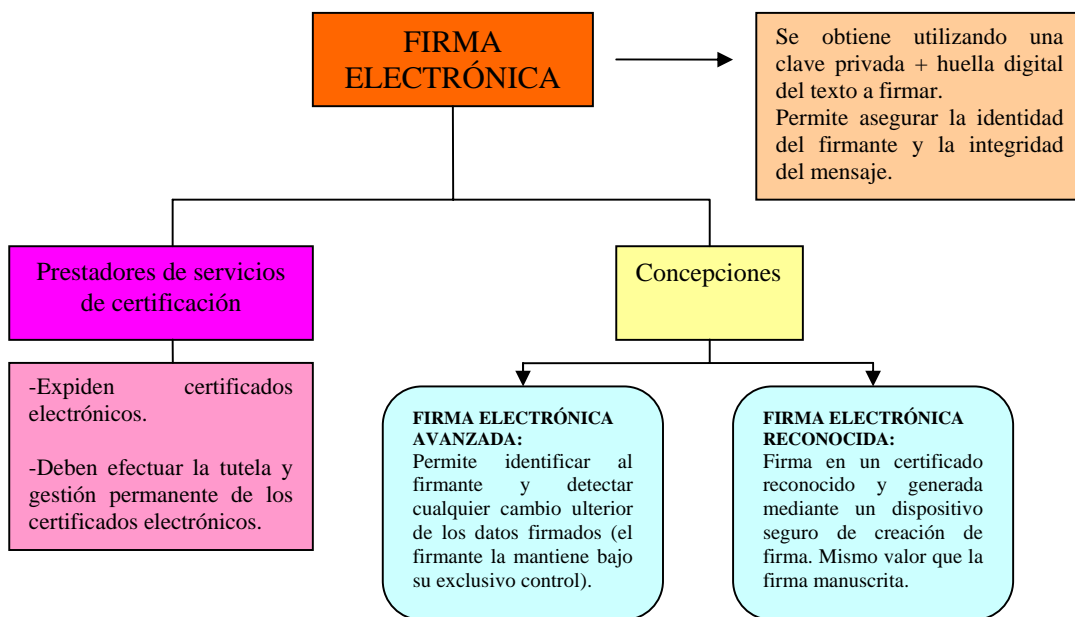
- a) **Documentos públicos**, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.
- b) **Documentos expedidos y firmados electrónicamente** por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.
- c) **Documentos privados**.

Los documentos a que se refiere el apartado anterior tendrán el **valor y la eficacia jurídica que corresponda a su respectiva naturaleza**, de conformidad con la legislación que les resulte aplicable.

El soporte en que se hallen los datos firmados electrónicamente **será admisible como prueba documental en juicio**. Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el **apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil**.

No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

Cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.



3. EMPLEO DE LA FIRMA ELECTRÓNICA EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS.

El uso de la firma electrónica se aplicará en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Las Administraciones públicas, con el objeto de salvaguardar las **garantías** de cada procedimiento, podrán establecer **condiciones adicionales a la utilización** de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por **fecha electrónica** el “conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.”

Las **condiciones adicionales** sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el **artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común**. Estas condiciones serán **objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación** al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

La utilización de la firma electrónica en las comunicaciones que afecten a la **información clasificada, a la seguridad pública o a la defensa nacional** se regirá por su **normativa específica**.

4. LOS CERTIFICADOS ELECTRÓNICOS.

Un **certificado electrónico** es un documento firmado electrónicamente por un **prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad**. Son como un DNI electrónico que garantizan en Internet la identidad de las personas.

El **firmante** es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Podrán solicitar certificados electrónicos de **personas jurídicas** sus administradores, representantes legales y voluntarios con poder bastante a estos efectos. Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario. Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

Son causas de **extinción** de la **vigencia de un certificado electrónico**:

- a. **Expiración del período de validez** que figura en el certificado.
- b. **Revocación** formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- c. **Violación o puesta en peligro del secreto de los datos** de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
- d. **Resolución judicial o administrativa** que lo ordene.
- e. **Fallecimiento o extinción de la personalidad jurídica** del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- f. **Cese en la actividad** del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
- g. **Alteración de los datos aportados** para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- h. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Los prestadores de servicios de certificación **suspenderán la vigencia de los certificados electrónicos** expedidos si concurre alguna de las siguientes **causas**:

- a. **Solicitud** del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- b. **Resolución judicial o administrativa** que lo ordene.
- c. La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c y g del **artículo 8.1 de la Ley 59/2003**.
- d. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se **incluya en el servicio de consulta** sobre la vigencia de los certificados del prestador de servicios de certificación.

La extinción o suspensión de la vigencia de un certificado electrónico **no tendrá efectos retroactivos**.

La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá **accesible en el servicio de consulta** sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

CERTIFICADOS RECONOCIDOS: 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.**”

Los certificados reconocidos incluirán, al menos, los siguientes **datos**:

- a. La indicación de que se expiden como tales.
- b. El código identificativo único del certificado.
- c. La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- e. La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
- f. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- g. El comienzo y el fin del período de validez del certificado.
- h. Los límites de uso del certificado, si se establecen.

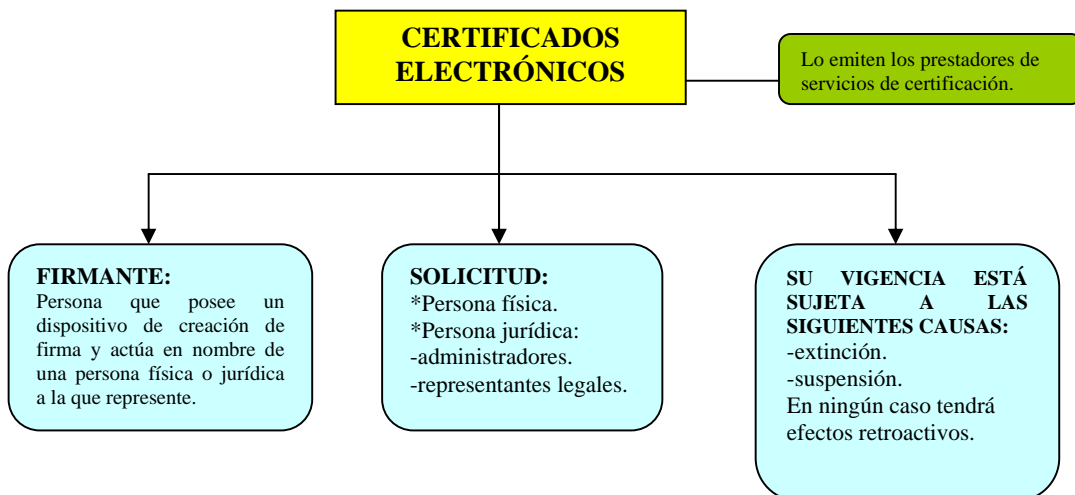
- i. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla las condiciones establecidas legalmente.

En el caso de **tramitación electrónica de procedimientos administrativos** la **dirección de correo electrónico incluida en el certificado** podrá ser utilizada por el destinatario de la solicitud para realizar los acuses de recepción y comunicar cualquier incidencia. No obstante, en el diseño de formularios de tramitación electrónica se prevé que el usuario pueda consignar otra dirección de correo distinta de la que consta en el certificado para notificaciones.



5. EL DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO.

El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la Ley 59/2003 impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la referida ley.

La Administración General del Estado empleará, en la medida de lo posible, sistemas que **garanticen la compatibilidad** de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

6. LA HUELLA DIGITAL.

Es un resumen del texto a firmar que se obtiene aplicando una función matemática denominada HASH y que da como resultado una cadena de caracteres de longitud fija y de tamaño inferior a texto original.

La función Hash se caracteriza por su irreversibilidad, es decir, no se puede construir el texto a firmar dada la función Hash y además tiene las siguientes propiedades:

- Dos textos iguales originan huellas digitales iguales.
- Dos textos parecidos originan huellas digitales diferentes. La probabilidad de que dos mensajes diferentes produzcan huellas digitales idénticas es prácticamente nula.

7. LA FIRMA DIGITAL.

La firma digital es un conjunto de datos asociados a un mensaje que permiten asegurar la identidad del firmante y la integridad del mensaje.

La firma digital no implica que el mensaje esté cifrado, esto es, un mensaje firmado será legible en función de que está o no cifrado.

El firmante generará mediante una función, un 'resumen' o huella digital del mensaje. Este resumen o huella digital la cifrará con su clave privada y el resultado es lo que se denomina firma digital, que enviará adjunta al mensaje original.

Cualquier receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación porque podrá generar el mismo resumen o misma huella digital aplicando la misma función al mensaje. Además podrá comprobar su autoría, descifrando la firma digital con la clave pública del firmante, lo que dará como resultado de nuevo el resumen o huella digital del mensaje.

Para poder realizar esta firma digital debemos solicitar un **Certificado de firma**.

Un **certificado** es *“un documento emitido y firmado por una Autoridad de Certificación basado en criptografía de clave asimétrica y que se compone básicamente de dos claves, una pública y otra privada ambas enlazadas mediante algoritmos matemáticos basados en la factorización de números primos”*. Además cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

Con la **Clave privada** vamos a poder firmar documentos y descifrar los documentos que nos cifran con nuestra clave pública.

Que para enviar documentos cifrados a otra persona, necesitamos la **clave pública** con la que ciframos los mensajes, que solo se pueden descifrarse con la clave privada relacionada en dicho certificado.

8. LA ADMINISTRACIÓN ELECTRÓNICA.

En materia de administración electrónica, corresponde a la **Inspección General de Servicios** las siguientes **funciones**:

- a. El análisis y validación funcional de cuantos sistemas y aplicativos informáticos se pretendan implantar en la Administración Pública de la Comunidad Autónoma de Canarias para la mejora del acceso de los ciudadanos a la Administración utilizando las tecnologías de la información y la comunicación, o que afecten al procedimiento administrativo común, entre ellos el sistema intercomunicado de registro e información administrativa al ciudadano entre las Administraciones públicas estatal, autonómica y local ("Ventanilla única"), firma electrónica y notificaciones telemáticas, conjuntamente con el centro directivo competente en materia de tecnologías de la información y de las comunicaciones.
- b. La dirección, organización y coordinación de la Web Institucional del Gobierno de Canarias, conjuntamente con el centro directivo competente en materia de tecnologías de la información y de las comunicaciones, sin

- perjuicio de las competencias que correspondan a la Presidencia del Gobierno.
- c. Promover e impulsar el cumplimiento de las normas relativas a la utilización de los procedimientos instrumentados a través de técnicas informáticas, electrónicas y telemáticas en la Administración Pública de la Comunidad Autónoma de Canarias, en colaboración con el departamento competente en materia de tecnologías de la información y de las comunicaciones.
 - d. Elaborar, conjuntamente con el centro directivo competente en materia de tecnologías de la información y de las comunicaciones y del competente en el área material afectada, los planes y programas, así como las normas precisas para la implantación de los procedimientos instrumentados a través de técnicas informáticas, electrónicas y telemáticas en la Administración Pública de la Comunidad Autónoma de Canarias.

9. CIBERCENTRO.

CiberCentro es el Centro Integral de Servicios (CIS) Telemáticos el Gobierno Canario.

Su **objetivo** es atender todos los aspectos, extremo a extremo, de la gestión de servicios telemáticos, ofreciendo un punto único de atención al usuario.

Se ha pretendido crear un Centro de Excelencia que:

- Se encargue de la "evolución tecnológica" del propio centro y de futuros proyectos.
- Planifique la "estrategia de futuro".
- Explote los datos de forma que aproveche la información subyacente.

Los **servicios** que presta son los siguientes:

A) GESTIÓN DE SISTEMAS:

- Operación y mantenimiento de las plataformas informáticas.
- Sistemas locales y remotos.
- Copias de seguridad.
- Estadísticas.
- Aplicaciones.
- Pruebas y evaluaciones.
- Política de seguridad.
- Prevención de fallos.

B) GESTIÓN DE DATOS:

- Mantenimiento y monitorización de la infraestructura de la red de datos.
- Equipos de red y líneas de comunicaciones.

- Análisis de red y futuras ampliaciones.
- Planificación de cambios.
- Pruebas y evaluaciones.

C) GESTIÓN DE VOZ:

- Operación y mantenimiento del sistema de comunicación vocal.
- Centrales Ibercom.
- Sistema de tarificación.
- Información de tarjetas de equipos.
- Estudio de posibilidades de ampliación de las centrales
- Estudio de numeración.
- Control de equipamiento existente.
- Grupos de operadoras.
- Petición de compra y configuración a Telefónica.

D) GESTIÓN DE MICROINFORMÁTICA:

- Asistencia telefónica para el uso de la ofimática y la microinformática.
- Instalación y configuración de hardware y software.
- Instalación y configuración de redes.
- Resolución de problemas.
- Planificación de recursos.
- Asistencia al usuario.

E) VENTAJAS:

- Economías de escala.
- Sinergias de utilización.
- Optimización de recursos humanos.
- Punto único de atención a usuarios.
- Integración de servicios.
- Gestión centralizada de inventarios y directorios.

F) TECNOLOGÍA EMPLEADA

- Firewall de alta generación.
- Estructura basada en redirectores y granjas de servidores.
- Alta disponibilidad.
- Escalabilidad.
- Ticketing para control de calidad.
- Intranet para el funcionamiento de CyberCentro.
- Sistema integrado de telefonía (CTI) para Call-Centers.