




BANCO INTERAMERICANO DE DESARROLLO
BANCO INTERAMERICANO DE DESENVOLVIMENTO

INTER-AMERICAN DEVELOPMENT BANK
BANQUE INTERAMERICAINE DE DEVELOPPMENT

FIRMA DIGITAL Y CONTRATOS ELECTRONICOS

Documento conceptual para la legislación en la Era de la Información

Iniciativa GLIN AMERICAS
Banco Interamericano de Desarrollo

Preparado por el grupo de trabajo:

Miguel Álvarez, Congreso Nacional, Guatemala
José Alejandro Ayala Meza, Congreso Nacional, Honduras
Graciela Chaves, Biblioteca del Congreso de la Nación, Argentina
Cecilia Garat, Cámara de Senadores, Uruguay
Erick Landaverde, Asamblea Legislativa, El Salvador
Ninoska López, Asamblea Nacional, Nicaragua
Gabriela López Fabregat, GLIN-URUGUAY , Cámara de Senadores, Uruguay
Ricardo Martínez, Asamblea Legislativa, El Salvador
Erick Fernando Medina, Congreso Nacional, Honduras
Renán Pascal, Cámara de Senadores, Uruguay

Con la colaboración de:

Guillermo S. Castillo, División de Tecnología de la Información para el Desarrollo,
Departamento de Desarrollo Sostenible, Banco Interamericano de Desarrollo

Noviembre 2005

Este documento ha sido preparado para presentar, desde una perspectiva parlamentaria, las oportunidades de mejora y trabajo posibles en los Poderes Legislativos de las Américas. El objetivo principal es proveer información básica que permita una mejor discusión y un marco conceptual para elaborar las propuestas necesarias, adaptadas a la realidad nacional.

Las interpretaciones, opiniones, alternativas y conclusiones expresadas en éste documento son enteramente responsabilidad de los autores y no deben ser atribuidas a las instituciones a las que estos perteneces, al Banco Interamericano de Desarrollo, sus organizaciones afiliadas, miembros de su Directorio Ejecutivo o países que representan.

ÍNDICE

FIRMA DIGITAL
Un Documento conceptual para legislación en la era de la Información

I.- INTRODUCCIÓN

La revolución tecnológica de finales del último siglo, especialmente en el campo electrónico y digital, trajo consigo un gran cambio en la forma de comunicación, de transmisión de la información, de trabajo y en general, ha afectado todas las actividades humanas. Este cambio ha impactado también en las estructuras jurídicas y ha puesto en crisis conceptos normativos pacíficamente aceptados por la doctrina y la jurisprudencia durante mucho tiempo, pero el derecho es evolutivo por naturaleza y debe adaptarse a los cambios y proveer a la sociedad del marco jurídico necesario para hacer relevante el uso de estas nuevas tecnologías.

GLIN-AMERICAS, iniciativa de la División de Tecnología de la Información para el Desarrollo, del Departamento de Desarrollo Sostenible, del Banco Interamericano de Desarrollo, y funcionarios de las Estaciones GLIN de los poderes legislativos de varios países de América Latina consideraron relevante abocarse al estudio de la legislación existente respecto de estas nuevas formas de comunicación y de comercialización a nivel mundial, el análisis de sus efectos en el corto plazo y la necesidad de contar con legislación actualizada que permita a los países de la región interactuar con un marco jurídico acorde.

El elemento base de este movimiento a nivel global, que permite el desarrollo del comercio internacional con una celeridad desconocida hasta ahora y brinda seguridad a las transacciones, es la firma digital y la certeza que de ella emana. La firma digital es ya una realidad y se usa en el mundo

Los países que han legislado en la materia equipararan la firma electrónica ó digital a la tradicional firma manuscrita u ológrafa, que tiene características propias, la principal de ellas es que es aceptada legalmente, esto quiere decir que si una persona firmó un documento adquiere tanto los derechos como las obligaciones que de él deriven, y si no cumple con obligaciones a su cargo, el tenedor del documento puede demandar judicialmente el cumplimiento. La autoridad competente acepta las responsabilidades adquiridas con sólo calificar a la firma como válida.

Existen, para la tradicional firma manuscrita dos etapas:

a) la primera el proceso de firma, que es el acto cuando una persona "firma" manualmente un documento. Esa firma generalmente es siempre igual y se usa como una marca personal; y
b) la segunda el proceso de verificación de la firma, que es el acto que determina si una firma es válida o no. La más común es la verificación visual, pero la legalmente definitoria es la pericia en laboratorio

Es importante recalcar que la firma comprueba la identidad de una persona, de tal modo que se sabe quién es la persona que firmó, y esa persona no puede negar las responsabilidades que adquiere en un documento firmado. Asimismo, muchas veces se recurre aun escribano ó notario público que certifica la autenticidad de la firma.

Es menester analizar si la firma digital aporta los mismos beneficios que la firma manuscrita en cuanto a su valor probatorio y a las responsabilidades civiles, penales, fiscales, etc. que pudieran derivar de los actos celebrados a través de estos nuevos instrumentos.

II.- DEFINICIONES

Al comenzar el análisis de este tema nos enfrentamos a un nuevo léxico con conceptos que se relacionan entre sí y pueden resultar confusos: criptografía simétrica, criptografía asimétrica, funciones matemáticas, clave privada, clave pública, autoridad de certificación, etc.

Por otra parte, los conceptos "firma electrónica" y "firma digital" no siempre son equivalentes en la legislación comparada, no obstante son usados en forma indistinta.

En efecto, en **Argentina** se entiende por ***firma electrónica*** al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital (artículo 5º Ley 25.506 de 14/11/2001). Esta definición legal obliga a averiguar que se considera firma digital y el artículo 2° de la misma ley, entiende por ***firma digital*** al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

En **Uruguay** el artículo 2ª, literal a) del decreto 382/03, de 17/9/2003 define la ***firma digital*** como el resultado de aplicar a un documento un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita, simultáneamente, identificar al firmante y detectar alteración del documento digital posterior a su firma.

Asimismo el Decreto 65/98 de 10/3/ 1998 define en su artículo 18 a la ***firma electrónica*** como "el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente a un individuo y a su voluntad de firmar" En el artículo 19 define a la ***firma digital*** como "un patrón creado mediante criptografía debiendo utilizarse sistemas criptográficos de clave pública o asimétrica o los que determine la evolución de la tecnología".

El artículo 3 de la Ley 27.269 de la legislación de **Perú**, de 4/5/2000, con la modificación del artículo 11 introducido por la Ley 27.310 de fecha 26/6/2001 define indistintamente ***firma electrónica o digital*** como aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública puedan derivar de ella la clave privada.

Costa Rica, en el artículo 8º de la Ley 8.454, de 23/8/2005 **"Ley de Certificados, Firmas Digitales y Documentos Electrónicos",** entiende por ***firma digital*** cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

Por otra parte, en **Ecuador** el artículo 13 de la Ley 67 del 17/4/2002, habla de ***firma electrónica***, con el mismo sentido que la ***firma digital***, definiéndola como los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba y reconoce la información contenida en el

mensaje de datos. Esta definición es coincidente con la del artículo 2º literal a) de la Ley Modelo para las Firmas Electrónicas, elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (**UNCITRAL**) del año 2001.

España, *el Real Decreto-Ley 14/1999 de 17 setiembre 1999*, derogado por la Ley 59 de 19/12/2003, en su artículo 3ª define a la ***firma electrónica*** como 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. ***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.

Chile la Ley 19.799 de 25 marzo 2002, define en su artículo 2º literal f), a la ***firma electrónica*** como cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor, y en el literal g) define a la ***firma electrónica avanzada*** como aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

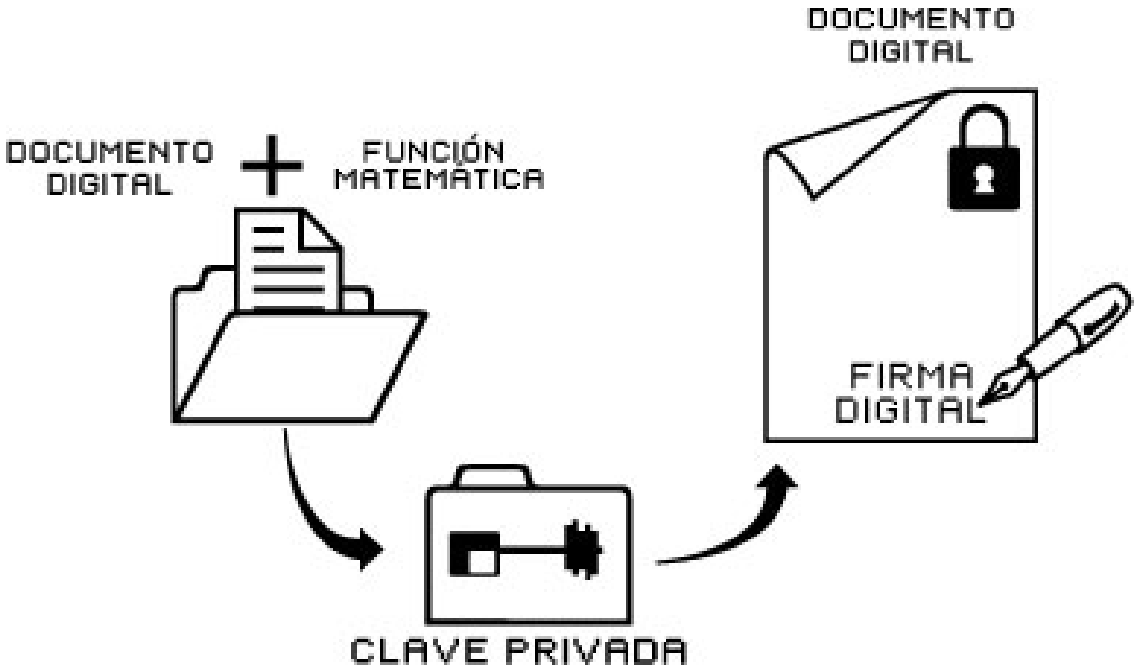
Brasil, se define la *firma electrónica* y se la distingue de la *firma electrónica avanzada* por producir ésta última mayores efectos y protección legal. Este fue también el criterio imperante en la **Unión Europea** según ***Directiva*** 1999/93/CE sobre el Marco Comunitario para la Firma Electrónica de 13 de diciembre de 1999.

Colombia define a la ***firma digital*** en el artículo 2º literal c) de la Ley 527 de 18/8/1999, como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto d l mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Panamá habla también indistintamente de firma electrónica y de firma digital ya que en la ley 43 de Firma Digital del 31/7/2001 define a la firma electrónica como todo sonido, símbolo, o proceso electrónico vinculado a o lógicamente asociado con un mensaje, y otorgado o adoptado por una persona con la intención de firmar el mensaje que permite al receptor identificar a su autor.

De todas las definiciones legales se puede concluir que la ***firma digital*** es un conjunto de datos adjuntados o asociados a un mensaje y utilizados como medio para identificar al autor y garantizar la integridad de los documentos digitales. Entonces, es el resultado de obtener un patrón que se asocie biunívocamente a un individuo y su voluntad de firmar, utilizando determinados mecanismos, técnicas o dispositivos electrónicos que garanticen que después no pueda negar su autoría.

El fin de la firma digital es el mismo que el de la firma ológrafa: Prestar conformidad y responsabilizarse con el documento firmado. No obstante de los conceptos que anteceden se desprende que hay distintos niveles de "confiabilidad" y/o de "seguridad" de la firma electrónica. La firma digital para Argentina y Uruguay, la firma electrónica avanzada conforme la Unión Europea, otorga una presunción "iuris tantum", salvo prueba en contrario, que proviene del suscriptor. En cambio, la validez de la firma electrónica debe ser probada por quien la alega.


DOCUMENTO
DIGITAL
DOCUMENTO
DIGITAL
FUNCIÓN
MATEMÁTICA
FIRMA
DIGITAL
CLAVE PRIVADA

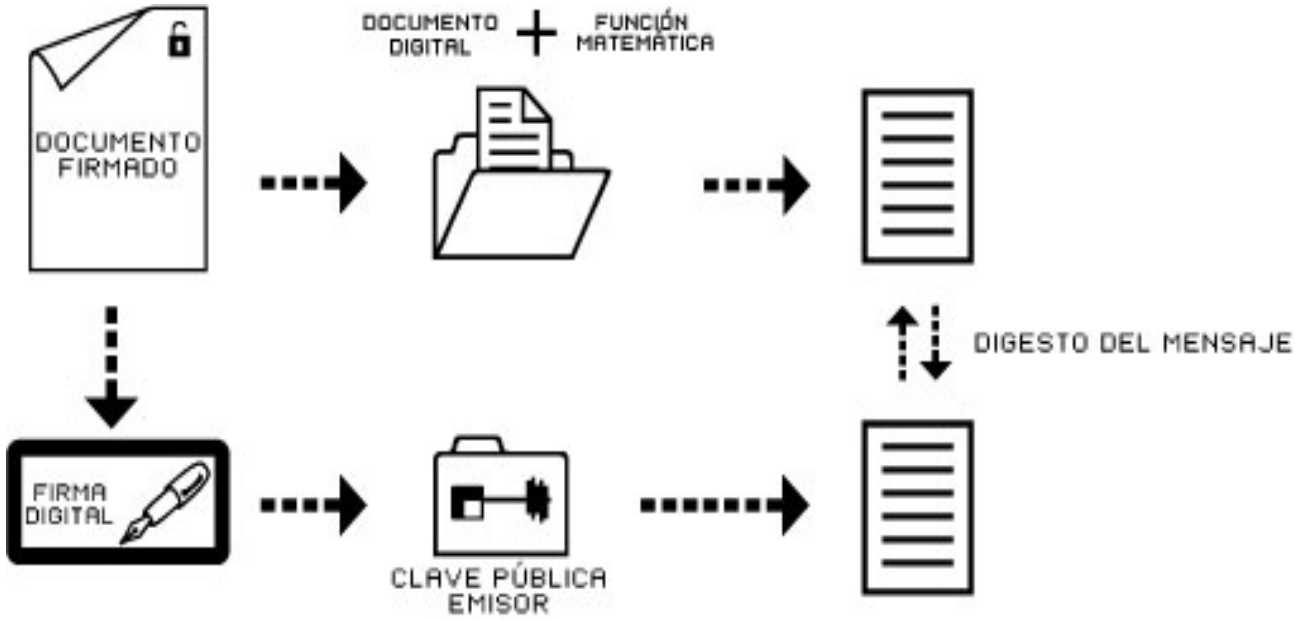
III.- ASPECTOS TÉCNICOS

El mecanismo de la firma digital debe cubrir los requerimientos y virtudes de una firma ológrafa en cuanto a la autenticación (permite identificar tanto al usuario que ha emitido el mensaje como al receptor); integridad del documento (asegura que el mensaje no ha sido alterado) y no repudio en virtud de que nadie excepto el emisor puede haberlo firmado y, en consecuencia, nadie podrá negar su existencia y validez legal.

La firma digital es un bloque de caracteres que acompaña a un documento o fichero acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrico), a la que sólo el tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

III.- 1. ¿Cómo se realiza una firma digital?

El software del firmante aplica un algoritmo hash sobre el texto a firmar, obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor. Los algoritmos hash más utilizados son el MD5 ó SHA-1. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits (según el algoritmo utilizado), se somete a continuación al cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA. De esta forma obtenemos un extracto final cifrado con la clave privada del autor, el cual se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.


DOCUMENTO DIGITAL
FUNCIÓN MATEMÁTICA
DOCUMENTO FIRMADO
DIGESTO DEL MENSAJE
FIRMA DIGITAL
CLAVE PÚBLICA EMISOR

III.- 2. ¿Qué es el CÓDIGO HASH?

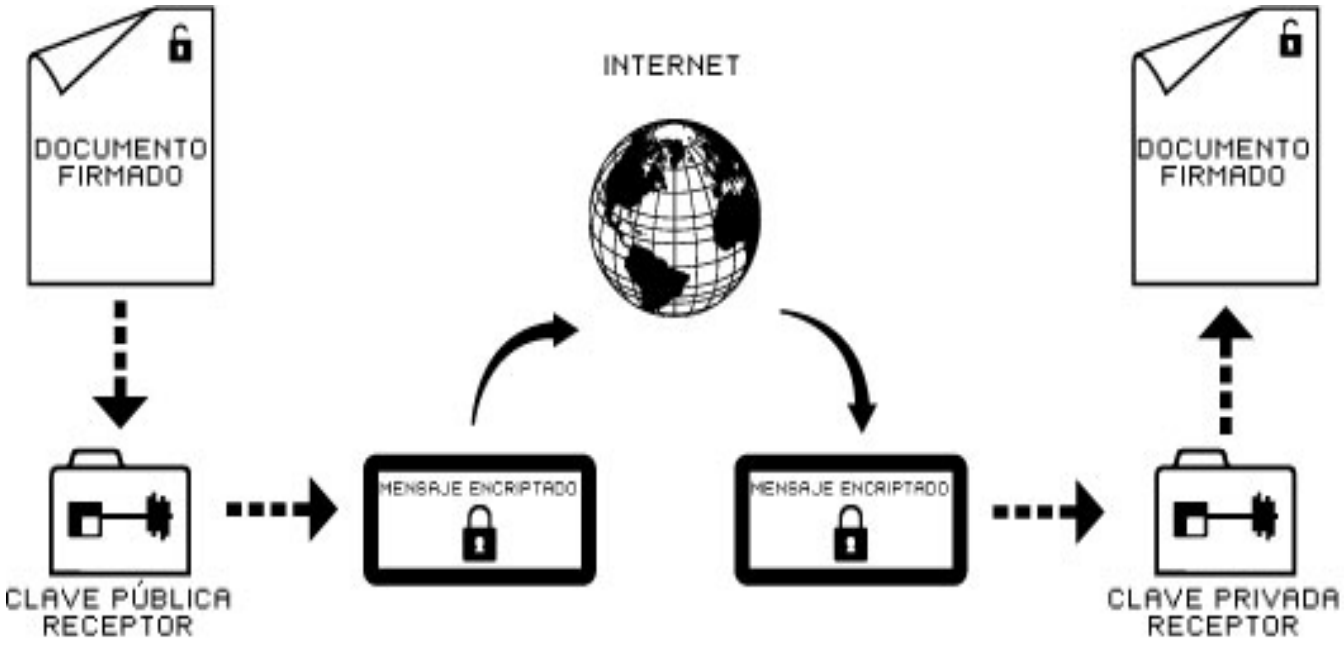
El sistema simétrico requiere, por una parte de un Tercero Proveedor de Servicios, que será quien facilite los equipos técnicos para efectuar las operaciones, y de una Autoridad Certificadora, que procederá a emitir un certificado, resumen o abstract que deberá cumplir con los requisitos legales sobre la firma digital o electrónica, en su caso, certificado que será el que normalmente se cifre y que genera un código único e inalterable, adjunto a la clave pública de una persona natural o jurídica, cuya función es garantizar que los datos contenidos en la clave están vigentes, son auténticos, están inalterados y corresponden a dicho persona natural.

Este certificado será el que estará cubierto con el código hash, que utiliza una función matemática consistente en crear una representación numérica para todo el certificado, de tal forma que éste pasa a ser representado por un valor numérico o cadena de datos.

Luego el originador procederá a codificar asimétricamente el certificado con la ayuda de su propia clave privada, enviando así el mensaje al destinatario. Este, una vez que lo recibe, procede a decodificar la firma electrónica con la ayuda de la clave pública. Como el destinatario sabe que el mensaje ha sido codificado con la clave privada del originador, le constará que éste es el autor del documento.

El sistema de firma electrónica opera de una forma inversa al envío del mensaje. Éste será codificado por el originador con su clave pública, y luego decodificado por el por el destinatario, con su clave privada. Con la *función Hash*, el certificado del texto quedará representado numéricamente. Generando un código que será su vez encriptado inversamente, con la clave privada del originador y luego desencriptado con la clave pública por el destinatario. Este certificado con *función hash* aplicada y luego codificado de manera inversa al documento, constituye la firma digital (1)

Con la aplicación de la *función hash*, cualquier cambio hecho en el texto, sea del certificado, sea del original, es previsto de inmediato, atendido que el código de ciframiento variará al cambiarse aunque sea una letra de uno u otro, lo que se verá cuando se comparen los textos con la correspondiente llave pública por pare del destinatario.


DOCUMENTO FIRMADO
INTERNET
DOCUMENTO FIRMADO
MENSAJE ENCRIPTADO
MENSAJE ENCRIPTADO
CLAVE PÚBLICA RECEPTOR
CLAVE PRIVADA RECEPTOR

III.- 3. ¿Cómo se comprueba la validez de la firma digital?
Para poder verificar la validez del documento o fichero es necesaria la clave pública del autor. El procedimiento sería el siguiente: el software del receptor, previa introducción en el mismo de la clave pública de remitente (obtenida a través de una Autoridad de Certificación), descifraría el extracto cifrado del autor y a continuación calcularía el extracto hash que le correspondería al texto del mensaje y, si el resultado coincide con el extracto anteriormente descifrado, se considera válida; en caso contrario significaría que el documento ha sufrido una modificación posterior y por lo tanto no es válido.

Últimamente se han dictado leyes dirigidas a otorgarle valor probatorio a la firma digital por ejemplo, la ley alemana sobre Signatura Digital; la Ley Italiana y su Reglamento, la Ley sobre Informática de la Federación Rusa, el decreto Argentino sobre firma digital en los actos internos del Sector Público, etc.

III.- 4. ¿Qué es la encriptación?

Existen básicamente dos tipos de encriptación

a) la criptografía simétrica que obliga a los dos interlocutores (emisor y receptor) del mensaje a utilizar la misma clave para encriptar y desencriptar el mismo (como por ejemplo el criptosistema DES, Data Encription Standard, desarrollado por IBM), y

b) la criptografía asimétrica o criptográfica de claves públicas que está basada en el concepto de pares de claves, de forma que cada uno de los elementos del par (una clave) puede encriptar información que solo la otra componente del par (la otra clave) puede desencriptar.

El par de claves se asocia con un solo interlocutor, así un componente del par (la clave privada) solamente es conocida por su propietario mientras que la otra parte del par (la clave pública) se publica ampliamente para que todos la conozcan (en este caso destaca el famoso criptosistema RSA cuyas iniciales son las de sus creadores: Rivest, Shamir y Adelman).

En la práctica la criptografía simétrica y asimétrica se usan conjuntamente. La simétrica por su rapidez, se utiliza para el intercambio de grandes volúmenes de información. La asimétrica para el intercambio de claves simétricas y para la firma digital.

IV.- CERTIFICADO DIGITAL

La firma digital requiere para su configuración de otros elementos tales como los Certificados Digitales. Estos certificados son documentos digitales, emanados de un certificador, que acreditan la vinculación entre una clave pública y una persona. Consiste en una estructura de datos firmados digitalmente por la autoridad certificadora, con información acerca de una persona y de la clave pública de la misma. Las entidades certificadoras emiten los certificados tras comprobar la identidad del sujeto.

El certificado permite realizar un conjunto de acciones de manera segura y con validez legal. Los certificados digitales son el equivalente digital del Documento de Identidad, en lo que a la autentificación de individuos se refiere, ya que permiten que un sujeto demuestre que es quien dice ser, es decir, que está en posesión de la clave secreta asociada a su certificado.

Todos los países que han legislado respecto de la firma digital establecen taxativamente las condiciones de validez de los certificados digitales, entre las que se encuentran:

Un identificador del propietario del certificado, que consta de su nombre y apellido, su dirección e-mail, localidad, provincia y país, etc.

Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.

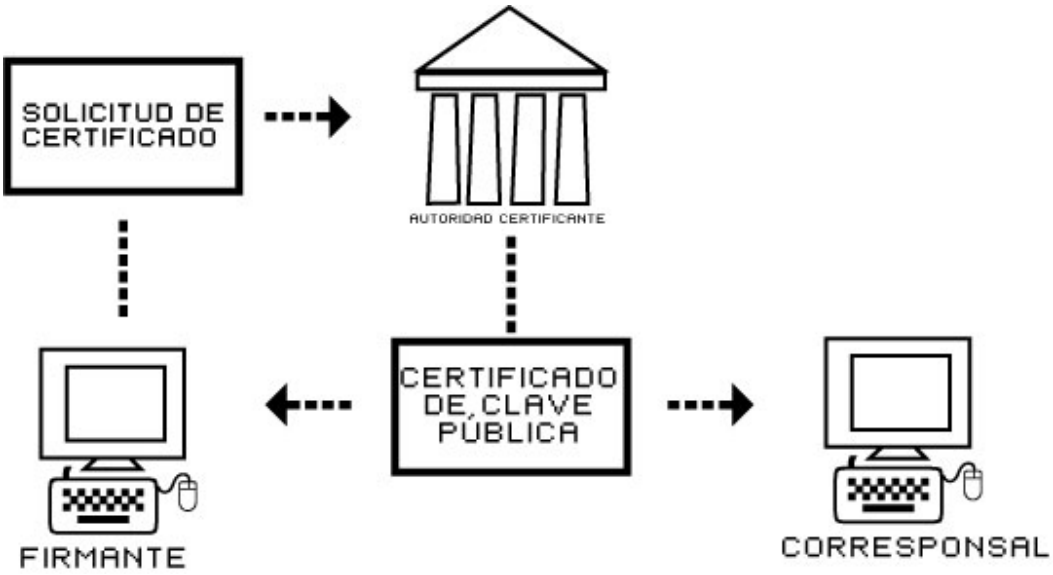
Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.

La firma de la Autoridad de Certificación que asegura la autenticidad del mismo.

Por lo tanto, los certificados digitales indican la autoridad certificadora que lo ha emitido, identifican al firmante del mensaje, contienen la clave pública del firmante, y contienen a su vez la firma digital de la autoridad certificadora que lo ha emitido.

Son, entonces, muy parecidos a un documento de identidad o a una certificación notarial y operan del siguiente modo: Se recibe un mensaje firmado; la clave pública del remitente viene cifrada y el mensaje es acompañado de un "Certificado" de la autoridad de certificación, cuya clave pública el receptor conoce. El receptor usa la clave pública de la tercera parte de confianza para verificar que el "Certificado" es auténtico; el certificado le señala a su vez que la clave pública del remitente es auténtica. Hecho esto, la utiliza para comprobar que la firma (o el documento) es auténtica.

Los certificados digitales emitidos por certificadores extranjeros son generalmente aceptados, con ligeras variantes, por la legislación de los distintos países. Así lo establece el Proyecto Modelo de UNCITRAL y la Directiva de la Unión Europea. Algunos países los aceptan a condición de reciprocidad establecida por acuerdo y cuando tales certificados sean reconocidos por un certificador licenciado en el país (Argentina). Otros sólo exigen que cumplan con los requisitos de la ley y tengan fiabilidad (Ecuador). Otra opción es requerir que un certificador nacional se haga responsabilice del certificador extranjero para autorizarlos por la autoridad competente (Perú).



Tipos de Certificados:

Autoridades de certificación Corporativas

Es la solución óptima para las empresas que quieran disponer de un sistema de generación de cualquier tipo de Certificado para sus usuarios (trabajadores, proveedores, clientes, etc.) y servidores. Una Autoridad de Certificación Corporativa puede generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código e incluso para IPSec-VPN. En función del tipo de funcionalidad que se le quiera dar a la CA se deberá escogerse un diferente tipo de CA Corporativa.

Certificados para firmar Código

El Certificado para la Firma de Código, permitirá a un Administrador, Desarrollador o Empresa de Software firmar su Software (ActiveX, Applets Java, Plug-ins, etc.) y Macros, y distribuirlo de una forma segura entre sus clientes.

V.- AUTORIDAD DE CERTIFICACIÓN

La Autoridad de Certificación (CA), es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real, asegurando su integridad y certificando la relación existente. Es la firma de la entidad de certificación la que garantiza que los certificados son validos, operan como escribanos que otorgan certificados de la firma pública de los solicitantes. Es decir que para brindar confianza a la clave pública surgen las autoridades de certificación, que son aquellas entidades que merecen la confianza de otros actores en un escenario de seguridad donde no existe confianza directa entre las partes involucradas en una cierta transacción. Es por tanto necesaria, una infraestructura de clave pública (PKI) para cerrar el círculo de confianza, proporcionando una asociación fehaciente del conocimiento de la clave pública o una entidad jurídica, lo que le permite la verificación del mensaje y su imputación a una determinada persona.

La confianza que los usuarios depositen en la Autoridad de Certificación es fundamental para el buen funcionamiento del sistema. El entorno de seguridad (control de acceso, cifrado, etc.) debe ser muy fuerte, en especial en lo que respecta a la protección de la Clave Privada que utiliza para firmar sus emisiones.

Las autoridades de certificación cumplen las siguientes funciones:

* Admisión de solicitudes. El usuario completa un formulario y lo envía a la autoridad de certificación solicitando un certificado.

* Autentificación del sujeto. Verificar la identidad del requirente antes de firmar la información proporcionada por el sujeto.

* Generación de certificados. Recibida la solicitud y validados los datos, la autoridad de certificación genera el certificado correspondiente y lo firma con su clave privada.

* Emisión de los certificados de usuarios registrados y validados por la Autoridad de Registro (RA).

·* Revocación de los certificados que ya no sean válidos (CRL - lista de certificados revocados). Un certificado puede ser revocado por que los datos han dejado de ser válidos, la clave privada se ha extraviado, ha sido robada o por cualquier otra razón ha dejado de ser privada o por fallecimiento de su titular, etc..

·* Renovación de certificados.

·* Publicar certificados en el directorio repositorio de certificados.

La emisión de certificados y la creación de claves privadas para firmas digitales depende de una pluralidad de entidades jerarquizadas de una manera que las de nivel inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Por último, existe una autoridad certificadora o licenciante que, generalmente pertenece al Estado.

En Uruguay el Decreto 382/03 de 17/9/2003 reglamenta el uso de la firma digital (reconocido por el art. 25 de la Ley 17.243 de 29 de junio de 2000) y el reconocimiento de su eficacia jurídica. Establece como definición de **Prestador de servicios de certificación**: "… tercera parte que expide certificados digitales, pudiendo prestar, además, otros servicios relacionados con la firma digital".

Los prestadores de servicios y firma digital según la tecnología de criptografía de clave asimétrica, que es la que refiere el Decreto 65/98 de 10/3/98 y reconocido por la posterior Ley 17.243 (Ley de Urgencia), requiere de la existencia de terceras partes que operen en calidad de prestadores de servicios como la certificación, información sobre las claves públicas y depósito de ellas, servicios de tecnología especialmente dedicada a la creación de programas de seguridad en firma digital.

El Proyecto de Ley de Uruguay. FIRMA DIGITAL. PRESTADORES SERVICIOS CERTIFICACIÓN. FUNCIONAMIENTO. REGULACIÓN de fecha 10/03/04, tratado en la Comisión de Constitución y Legislación de la Cámara de Senadores y archivado el 14 /2/2005, recoge los principios establecidos en el art. 25 Ley 17.243, de 29/6/2000, que dice textualmente: "*Autorízase en todo caso la firma electrónica y la firma digital, las que tendrán idéntica validez y eficacia a la firma autógrafa, siempre que estén debidamente autenticadas por claves u otros procedimientos seguros, de acuerdo a la tecnología informática*".

También reglamenta en el Título II, explicitando que se trata de una actividad que no está sujeta a autorización previa, pero se requiere el registro de quienes la desempeñen; crea un Registro de Prestadores de Servicios de Certificación de Firma Digital y establece los recaudos que deben cumplir las entidades que certifiquen firmas digitales. El contralor de las entidades de certificación registradas estará bajo la superintendencia de URSEC al solo efecto de supervisar el cumplimiento de las normas legales.

Detallan las funciones y obligaciones de los de servicios de certificación de firma digital, consagra el régimen de responsabilidad, frente a terceros, de las entidades certificadoras y define el concepto de infracción administrativa y el régimen de sanciones que URSEC podrá imponer a los prestadores infractores.

En suma, se entiende que la ley se limita a exigir a los prestadores de servicios, entre las obligaciones previas a la expedición de certificados reconocidos, la de comprobar la identidad y circunstancias personales de los solicitantes de certificados pero no les obliga a identificar a los firmantes de los documentos electrónicos e en que la firma se emplee, ni podría hacerlo, porque como señala RODRIGUEZ ADRADOS, se trata de hechos futuros, incontrolables por los proveedores de servicios de certificación.

La función de los prestadores de servicios de certificación es esencial ya que la firma digital debe encontrarse vigente al momento de la firma del documento, hecho que acreditan los certificados emitidos por estos prestadores de servicios, a efectos de que el documento así firmado no pueda ser repudiado.

Existen diferentes tipos de certificados con diferente vigencia en el tiempo o por diferentes valores y deben contener datos individualizantes del firmante que surgen de las distintas reglamentaciones o legislaciones al respecto.

Asimismo los prestadores de servicios deben ofrecer información a los usuarios respecto a la vigencia de los certificados y de las firmas digitales, como de las claves públicas, como forma de garantizar la contratación. Operarían como verdaderas Autoridades o Registros Públicos, por lo que en muchos casos se les denomina Autoridades Certificantes, aun cuando fueren entidades privadas.

De esta forma la firma digital podría brindar las mismas garantías en cuanto a autoría e integridad del mensaje, y si la tecnología empleada es la adecuada, su función resulta equivalente a la de la firma manuscrita, no pudiendo el firmante repudiarla.

En **Argentina** la Ley 25.506 de 14 noviembre 2001 en el Capítulo III establece que el certificador licenciado es toda persona de existencia ideal, registro público de contratos un

organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. Este ente licenciante es la Oficina Nacional de Tecnologías de Información que depende del Poder Ejecutivo, a través de la Jefatura de Gabinete de Ministros.

La actividad de los certificadores licenciados no pertenecientes al sector público, se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos. Hasta la fecha, según información de la Oficina Nacional de Tecnologías de la Información, no hay certificadores licenciados.

En **España**. El Real decreto 14/99 de 17 setiembre de 1999 sobre firma electrónica establece la prestación de servicios de certificación dentro de un régimen de libre competencia. Cuenta con un Registro de Prestadores de Servicios de Certificación y una Autoridad Pública de Certificación Española (CERES)

Las Agencias de Certificación españolas son:

1. Fábrica Nacional de Moneda y Timbre.
2. ACE (Agencia de Certificación electrónica)
3. FESTE. Está formado por el Consejo General del Notariado, el Consejo General de la Abogacía y la Universidad de Zaragoza.
4. IPSCA . Serivicios de firma electrónica y certificación digital.
5. CAMERFIRMA. Es la autoridad de certificación digital de la Cámara de Comercio españolas además de tener experiencia en servicios de out sourcing de Entidades de Certificación.

Existen algunas otras entidades de certificación de ámbitos locales y sectoriales, así como administraciones autonómicas.

Con respecto a Perú la Ley 27. 269 de 4 mayo de 2000 detalla las funciones de las entidades de Certificación y de Registro, acepta el régimen de libre competencia. En la reglamentación designa como autoridad de aplicación facultada para autorizar a las entidades de certificación al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual.

VI- INFRAESTRUCTURAS DE CLAVE PÚBLICA

Una infraestructura de clave pública (Public Key Infrastructure en inglés) es la combinación de productos de hardware y software, políticas y procedimientos para proveer un nivel adecuado de seguridad en transacciones electrónicas a través de redes públicas, como Internet.

La infraestructura de clave pública se basa en identificaciones digitales, también conocidas como "certificados digitales", los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública.

Debido a la característica impersonal involucrada en este tipo de tecnología – sin intercambio de documentos – es que se hace necesario contar con medios que garanticen una efectiva identificación y autenticación de los usuarios participantes con el fin de poder lograr el no repudio de las operaciones realizas. Asimismo, en todo momento debe poder ser garantizada la confidencialidad e integridad de las transacciones que viajan por la red.

Generalmente, una estructura de PKI consiste en:

- Una política de seguridad
- Una Autoridad Certificante
- Un sistema de administración de certificados
- Un conjunto de aplicaciones que hacen uso de la tecnología PKI

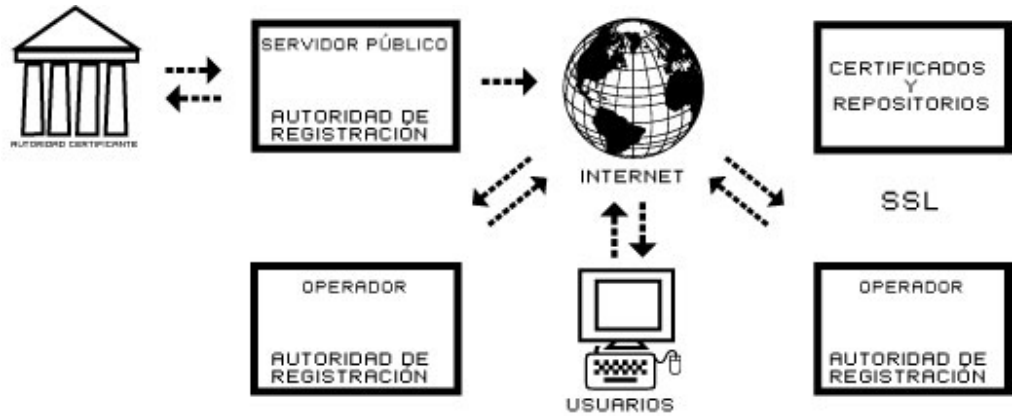
A continuación se describe brevemente cada una de las funciones desarrolladas por los componentes de la estructura;

- La política de seguridad establece y define la dirección que debería seguir la organización respecto de la seguridad de su información considerando también los procesos y principios establecidos para el uso de medios criptográficos. También incluye documentos de cómo la organización deberá manejar sus claves a fin de establecer el nivel de control deseado de acuerdo a los riesgos existentes. Típicamente, todos estos aspectos son agrupados en lo que es conocido como Certificate Practice Statements – CPS – Este documento es donde se detallan los procedimientos operacionales, como son el funcionamiento de la autoridad certificante, las actividades de administración de los certificados, las características de los certificados, etc.

- La autoridad certificante es el componente clave de una estructura PKI y es la encargada de realizar la emisión y administración de los certificados durante todo el ciclo de vida de los mismos.

- El sistema de administración de certificados y distribución establece el tratamiento que recibirán los certificados generados, desde el procedimiento de generación hasta su revocación o recerfiticación (solo si estuvo suspendido) y la manera en que serán distribuidos los certificados.

- El conjunto de aplicaciones PKI que hacen uso de la tecnología de clave pública, como ser comunicaciones entre un servidor Web, navegadores, correo electrónico y VPN.



Esta infraestructura de clave pública consta de una serie de autoridades que se especialicen en papeles concretos:

Autoridades de certificación (CA o certification authorities): que vinculan la clave pública a la entidad registrada proporcionando un servicio de identificación .Una CA es a su vez identificada por otra CA creándose una jerarquía o árbol de confianza: dos entes pueden confiar mutuamente entre sí a una autoridad común que directa o transitivamente las avala.
Autoridades de registro (RA o registration authoritites): que ligan entes registrados a figuras jurídicas, extendiendo la accesibilidad de las CA.

Autoridades de fechado digital (TSA o time stamping authorities): que vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado (resolverían el problema de la exactitud temporal de los documentos electrónicos).

Estas autoridades pueden materializarse como entes individuales, o como una colección de servicios que presta una entidad multipropósito.

Autenticación e integridad.

- La autenticidad se refiere a que cuando la entidad emisora envía la información a la entidad receptora, este última puede estar segura que el mensaje lo originó la entidad emisora original.
- La integridad se refiere a que la entidad receptora está segura de que la información que recibe de la entidad emisora no ha sido modificada desde que ésta la envió.

A pesar de que desde el punto de vista teórico se establece una distinción entre autenticación e integridad, los esquemas y algoritmos usados normalmente proporcionan ambos tipos de protección de forma combinada. Hay criterios que deben cumplir un algoritmo de autenticación e integridad.

El criterio básico de autenticidad tiene el propósito de evitar ataques normalmente basados en el criptoanálisis. Los mecanismos de autenticación e integridad tienen el propósito de detectar la actuación de una tercera entidad atacante activa.

VII.- CONTRATOS ELECTRONICOS

Intimamente relacionados con la firma digital, que contribuye a darles seguridad, están los contratos electrónico que debido al vertiginoso desarrollo de nuevas tecnologías, han surgido como nuevas estrategias de comercialización. Las empresas ofrecen sus productos a un mercado universalizado por Internet y los usuarios o consumidores tienen la posibilidad de acceder a una amplia gama de oferentes, que les permiten comparar y optar por lo que les resulta más conveniente.

Las características principales del contrato electrónico son:

1.- Las operaciones se realizan a través de medios electrónicos;

2.- El lugar donde se encuentren las partes resulta irrelevante;

3.- No queda registro en papel;

4.- Se reducen considerablemente los tiempos para efectivizar las transacciones;

5.- Se reducen los intermediarios de distribución;

6.- Las importaciones no pasan, necesariamente, por las aduanas

Esta última característica nos lleva a una clasificación doctrinaria de los contratos electrónicos que los divide en

a) Contratos electrónicos directos que son aquellos en los cuales el cumplimiento de la obligación contractual se hace a través de Internet (on line).

b) Contratos electrónicos indirectos, en los cuales el objeto de la prestación es un bien material o un servicio que debe ejecutarse fuera de la red. (off line).

Por otra parte, atento los sujetos que sean parte del contrato, pueden clasificarse:

a) Business to Business (B2B), contratos celebrados entre empresas

b) Business to Consumers (B2C), contratos celebrados entre las empresas y sus consumidores

c) Business to Government (B2G), contratos a través de portales de compra estatales

Es indudable que el comercio mundial ha cambiado. En un mundo basado en redes han desaparecido las barreras temporales, en pocos segundos la información recorre el planeta, y también han desaparecido las barreras geográficas y jurídicas. Los contratos electrónicos han surgido más allá de la existencia o no de una legislación al respecto, y han alcanzado importantes niveles a escala mundial. El derecho de los contratos deberá adaptarse al nuevo entorno.

Los juristas se encuentran aplicando analógicamente las doctrinas tradicionales a un derecho nuevo. La globalización genera una especie de extraterritorialidad de los intercambios económicos pero la seguridad del comercio requiere siempre del contrato como instrumento jurídico básico.

Al hablar de contratos nos referimos al acuerdo de voluntades en orden a una determinada convención destinada a reglar sus derechos. Se fundamenta principalmente en la autonomía de la voluntad de las partes. Pero en el mundo de Internet, las nuevas estrategias de contratación y

los contratos electrónicos no son más que un acuerdo de voluntades, aunadas a través de redes digitales, destinadas a crear, modificar o transferir derechos de las partes.

Aparentemente, un contrato electrónico no es más ni menos que un contrato que se realiza utilizando medios electrónicos a través de la red.

Sin perjuicio de lo expuesto, se presentan como una realidad distinta, el acuerdo de voluntades no se ve plasmado en un documento papel con la firma autógrafa de las partes y esto obliga a los estudiosos a analizar este nuevo fenómeno que genera el comercio electrónico.

El primer antecedente de legislación respecto del comercio electrónico, y por ende de los contratos electrónicos, lo elaboró la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en el año 1996, a través de la Ley Modelo para el Comercio Electrónico "con objeto facilitar el uso de medios modernos de comunicación y de almacenamiento de información", y que "proporciona los criterios para apreciar el valor jurídico de los mensajes electrónicos". Ofrece un conjunto de normas claras aceptables internacionalmente y ha resultado de ayuda para la formación de legislaciones nacionales.

Hasta la fecha han utilizado, con ligeras variantes, la Ley Modelo de la CNUDMI los siguientes países Latino Americanos: Colombia, Ecuador, México Panamá, República Dominicana y Venezuela.

VII.- 1. Consentimiento

Como todo contrato el "contrato electrónico" toma forma a partir del consentimiento y la ausencia de fronteras obliga a analizar el lugar de celebración que a su vez determinará la ley aplicable y la jurisdicción competente en caso de conflicto.

La Convención de Viena de 1998 sobre Compraventa Internacional de Mercaderías establece que el contrato se perfecciona cuando llega al oferente la notificación de la aceptación. En los contratos electrónicos, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, en la Ley Modelo para el Comercio Electrónico y el derecho comparado, en general, aceptan pacíficamente que el contrato queda perfeccionado en el momento que la aceptación ingresa al sistema informático del oferente. No es necesario que el oferente tenga conocimiento de la aceptación. Basta que ingrese en su esfera de control. Se establece además, la obligación a cargo del oferente de emitir un "acuse de recibo" de la aceptación para dar seguridad a las transacciones comerciales.

VII.- 2. Jurisdicción competente y Ley aplicable

En el ámbito de la Comunidad Europea, el Reglamento 44/2001 y los Convenios de Bruselas y Lugano, establecen el principio de autonomía de la voluntad. Las partes pueden determinar libremente el lugar de celebración del contrato y establecer así la ley aplicable y la jurisdicción competente a la que se someterán en caso de litigio. Esta solución es recomendable cuando se trata de una contratación entre empresas que cuentan con una capacidad de negociación similar, así la competencia queda determinada en el mismo momento de la formación de contrato.

Ante la falta de un pacto de sumisión, la normativa citada, prevee dos posibilidades

1.- Recurrir a la Justicia en el Estado en que tenga su domicilio el demandado

2.- Demandar en los Tribunales del Estado en que debió cumplirse la obligación objeto de la demanda

En el primer caso, en el ámbito de los contratos electrónicos, puede resultar difícil determinar el domicilio de demandado, si este no está debidamente identificado. En segundo supuesto, presenta problemas cuando se tratan de contratos electrónicos directos o de cumplimiento on line.

Al respecto, la doctrina ha elaborado diferentes soluciones: el lugar donde el destinatario tiene la sede principal de su negocio ó actividad, el lugar donde se encuentra el registro en el cual está obligado a inscribirse el oferente y por último el lugar donde está ubicado el servidor a través del cual se celebró el contrato.

VII.- 3. Contratos B2C

No es igual la situación del consumidor que no está, en principio, en condiciones de internacionalizar sus contratos ó someterse a jurisdicciones extrañas.

Cuando se trata de contratos con consumidores, toda la normativa tiende a la protección del consumidor y, por lo tanto, se consideran celebrados en el lugar donde este tenga su domicilio habitual, así no podrá verse perjudicado o privado de la protección que le garantiza la ley del país en que reside ni del acceso a la jurisdicción.

No es casual que todas las legislaciones tiendan a dar seguridad a los consumidores dentro de este inmenso mercado que es el comercio electrónico. En efecto, son los millones de consumidores los que hacen crecer esta nueva forma de comercio mundial que permite el acceso a los más variados servicios y a un enorme universo de bienes.

VIII.- ESTADO ACTUAL Y TECNOLÓGICO EN AMÉRICA LATINA Y EN EL MUNDO

La Sociedad de la Información y las Tecnologías de la Información y la Comunicación requieren una planificación por parte del Estado, no solo por la importancia que tienen en el plano económico sino también en cuanto al diseño y aplicación de políticas sociales igualitarias en acceso a la información y al conocimiento. La globalización que se presenta como oportunidad para el desarrollo no es más que la adaptación de los sistemas productivos a la lógica capitalista, donde la innovación tecnológica viene a asegurar y reproducir el modelo de producción. No obstante la falta de adecuación de los países al mismo los deja en posiciones marginales, dependientes del desarrollo científico y técnico y condenados a la producción de materias primas con escaso valor agregado.

Unos 685 millones de personas, o sea, el 11% de la población mundial, tenía acceso a Internet en 2003.

Más de la tercera parte de los usuarios de Internet viven en países en desarrollo, cuya proporción en la "población de Internet" del mundo aumentó en casi el 50% entre 2000 y 2003.
Cinco países (Brasil, China, la India, México y la República de Corea) representan más del 60% del total de usuarios de Internet del mundo en desarrollo.

El total mundial de anfitriones de Internet aumentó en un 35,8% de enero de 2003 a enero de 2004, elevándose a más de 233 millones, aumento que duplicó con creces el de 2002. La mayoría de los anfitriones pertenecen a dominios genéricos de alto nivel, como .net o .com, que no pueden asociarse a una ubicación geográfica determinada, por lo que resulta difícil determinar el número absoluto y relativo de anfitriones de cada país. Pero en enero de 2003 los únicos dominios genéricos de alto nivel correspondientes a países en desarrollo que se ubicaban entre los 40 primeros por el número de anfitriones eran los de Brasil (.br), la Provincia china de Taiwán (.tw), México (.mx), Argentina (.ar), la República de Corea (.kr), Hong Kong, China (.hk) y Singapur (.sg).

En enero de 2004 los dominios genéricos de alto nivel de Turquía (.tr) y Sudáfrica (.za) se habían sumado a los 40 primeros del Internet Domain Name Survey del Internet Software Consortium (ISC).

Los sitios web constituyen las principales pasarelas a Internet tanto para las transacciones entre empresas y consumidores como para las transacciones entre empresas, por lo que la evolución del número de servidores web en el mundo es un indicador útil del crecimiento del sector de las transacciones electrónicas. En junio de 2004 había más de 51.635.000 sitios web en el mundo, según una encuesta de Netcraft.com, cifra que representaba un 26,13% de aumento respecto al mismo mes de 2003. Los 10,7 millones de nuevos sitios añadidos a la red en sólo un año ponen de manifiesto una importante aceleración, habida cuenta de que la red necesitó 21 meses para crecer de 30 a 40 millones de sitios. El número de sitios activos, o sea, los que permiten la interactividad de los usuarios, aumentó un poco más (26,39%) en los 12 meses anteriores a junio de 2004.

El número de sitios web que utilizan el protocolo de capa de protección segura (Secure Socket Layer, SSL), que posibilita la seguridad de las transacciones, aumentó en un 56,7% en los 12 meses del período abril de 2003 a abril de 2004, llegando a 300.000, según otra encuesta de Netcraft, lo que de alguna manera refleja la utilización de la red para las transacciones comerciales, a pesar de que el SSL no se usa exclusivamente con ese fin.

Apenas el 1 % de la inversión mundial en investigación y desarrollo tecnológico se dirige a los países latinoamericanos, esto revela un dramático retraso de América Latina respecto de China, India y los países de la ex Europa del Este. Sin investigación tecnológica, los países no pueden producir bienes de mayor valor agregado, que puedan ser exportados al resto del mundo a precios

más altos. A menos que esto cambie, América Latina estará condenada a seguir exportando materias primas.

La división del mundo en países ricos y países pobres, se ha acentuado cada vez más y lo más sorprendente es que no se debe a la concentración de los factores de producción, como el capital o el trabajo, sino más bien a factores relativos al conocimiento. Los países ricos han generando nuevas tecnologías, que explican su crecimiento económico. El ingreso promedio per cápita anual en los países ricos supera en un 75% el nivel de ingresos en la región de América Latina y el Caribe y gran parte de esa diferencia ocurrió durante el último cuarto de siglo.

La globalización ha profundizado las diferencias y aumentó las desigualdades entre nuestros países y los otros. Pero también **entre** nuestros países latinoamericanos y **dentro** de cada uno de nuestros propios países. La población que accede a Internet, en América Latina es una porción muy reducida. En Perú y El Salvador se han implementado cabinas públicas, en Argentina, Ciber-cafés, que permiten el uso de computadoras conectadas a Internet mediante el pago de una cantidad relativamente reducida. Chile también ha desarrollado programas tendientes a extender el uso de computadoras a la población.

Revertir esta situación requiere una intervención gubernamental que aliente la inversión en investigación tecnológica de alto y estimule la oferta y demanda de tecnología nacional, con programas tipo "compre nacional" y privilegiando la exportación de tecnología con importantes incentivos e incluso el acceso al crédito ó a subsidios. Básicamente, es necesario legislar, someter estos temas al debate, habida cuenta que se ha demostrado el crecimiento del comercio electrónico en aquellos países que han legislado al respecto.

Por último, y no menos importante, favorecer la educación digital en las escuelas públicas y promover la capacitación permanente de los adultos mediante sistemas de reintegro de impuesto ó exenciones impositivas.

IX.- GLOSARIO

Autoridad Certificante (CA, por su denominación en inglés): Organización o entidad de confianza encargada de emitir, registrar y publicar certificados. Además verifica la identidad del solicitante del certificado y publica las listas de revocación de certificados. También son las encargadas de mantener los registros de claves públicas directamente en línea (on line).

Certificado digital: Registros electrónicos que atestiguan fehacientemente que determinada clave pública pertenece a una persona o entidad, permite realizar un conjunto de acciones de manera segura y con validez legal.

Cifrado de claves pública y privada: Es una forma asimétrica de cifrado basado en un par de claves, pública y privada, generadas criptográficamente. Los datos cifrados con una clave privada pueden descifrarse únicamente con la clave pública correspondiente y viceversa.

Clave: Valor utilizado en combinación con un algoritmo para encriptar o desencriptar información. Los algoritmos de cifrado simétricos utilizan la misma clave para cifrar y descifrar mientras que los algoritmos asimétricos utilizan un par de claves: pública y privada.

Clave privada y clave pública: Mitad del secreto de un par de claves: pública y privada. Se utilizan para firmar digitalmente un mensaje o descifrarlo.

Código Hash: Utiliza una función matemática consistente en crear una representación numérica para todo el certificado, de tal forma que éste pasa a ser representado por un valor numérico o cadena de datos.

Firma digital: Herramienta tecnológica que se incluye o transmite con un mensaje y se utiliza para identificar y autentificar al emisor y a la información del mensaje y así garantizar su validez, integridad e invariabilidad de los datos durante el tránsito.

Firma electrónica: Conjunto de datos electrónicos adjuntados o asociados a un mensaje y utilizados como medio para identificar al autor con relación al mismo e indicar que lo aprueba.

Firma electrónica avanzada: Denominación equivalente a la "firma digital" utilizada por algunas legislaciones, como es el caso de España, la Unión Europea, Brasil y Chile.

Infraestructura de Clave Pública: Conocida mundialmente con las siglas PKI por su denominación en inglés Public Key Infraestructure, es al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes.

Par de claves: Formado por una clave pública y otra privada pertenecientes a una entidad y utilizadas para cifrar y descifrar datos.

ANEXO LEGISLACIÓN.

ARGENTINA

Ley 25.506

Sancionada: Noviembre 14 de 2001.

Promulgada de Hecho: Diciembre 11 de 2001.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

LEY DE FIRMA DIGITAL

CAPITULO I

Consideraciones generales

ARTICULO 1º — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4º — Exclusiones. Las disposiciones de esta ley no son aplicables:

a) A las disposiciones por causa de muerte;

b) A los actos jurídicos del derecho de familia;

c) A los actos personalísimos en general;

d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8º — Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9º — Validez. Una firma digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTICULO 10. — Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II

De los certificados digitales

ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

a) Ser emitidos por un certificador licenciado por el ente licenciante;

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:

1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

2. Ser susceptible de verificación respecto de su estado de revocación;

3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;

4. Contemplar la información necesaria para la verificación de la firma;

5. Identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15. — Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16. — Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o

b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

CAPITULO III

Del certificador licenciado

ARTICULO 17. — Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

ARTICULO 18. — Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19. — Funciones. El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20. — Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21. — Obligaciones. Son obligaciones del certificador licenciado:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;

q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

ARTICULO 22. — Cese del certificador. El certificador licenciado cesa en tal calidad:

a) Por decisión unilateral comunicada al ente licenciante;

b) Por cancelación de su personería jurídica;

c) Por cancelación de su licencia dispuesta por el ente licenciante.

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23. — Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

a) Para alguna finalidad diferente a los fines para los cuales fue extendido;

b) Para operaciones que superen el valor máximo autorizado cuando corresponda;

c) Una vez revocado.

CAPITULO IV

Del titular de un certificado digital

ARTICULO 24. — Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;

c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;

d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25. — Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V

De la organización institucional

ARTICULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27. — Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

ARTICULO 28. — Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

CAPITULO VI

De la autoridad de aplicación

ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

ARTICULO 30. — Funciones. La autoridad de aplicación tiene las siguientes funciones:

a) Dictar las normas reglamentarias y de aplicación de la presente;

b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;

c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;

d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;

e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;

f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;

g) Determinar los niveles de licenciamiento;

h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;

i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;

j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;

k) Aplicar las sanciones previstas en la presente ley.

ARTICULO 31. — Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;

b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;

c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;

e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.

ARTICULO 32. — Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto.

CAPITULO VII

Del sistema de auditoría

ARTICULO 33. — Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoría por sí o por terceros habilitados a tal efecto. Las auditorías deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

ARTICULO 34. — Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorías las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

CAPITULO VIII

De la Comisión Asesora para la Infraestructura de Firma Digital

ARTICULO 35.— Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36. — Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

a) Estándares tecnológicos;

b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;

c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;

d) Metodología y requerimiento del resguardo físico de la información;

e) Otros que le sean requeridos por la autoridad de aplicación.

CAPITULO IX

Responsabilidad

ARTICULO 37. — Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

ARTICULO 38. — Responsabilidad de los certificadores licenciados ante terceros.

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

ARTICULO 39. — Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X

Sanciones

ARTICULO 40. — Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

ARTICULO 41. — Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

a) Apercibimiento;

b) Multa de pesos diez mil ($ 10.000) a pesos quinientos mil ($ 500.000);

c) Caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación.

El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42. — Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;

b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;

c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43. — Multa. Podrá aplicarse sanción de multa en los siguientes casos:

a) Incumplimiento de las obligaciones previstas en el artículo 21;

b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;

c) Omisión de llevar el registro de los certificados expedidos;

d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;

e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorías por parte de la autoridad de aplicación y del ente licenciante;

f) Incumplimiento de las normas dictadas por la autoridad de aplicación;

g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.

ARTICULO 44. — Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

a) No tomar los debidos recaudos de seguridad en los servicios de certificación;

b) Expedición de certificados falsos;

c) Transferencia no autorizada o fraude en la titularidad de la licencia;

d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;

e) Quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45. — Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46. — Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

CAPITULO XI

Disposiciones Complementarias

ARTICULO 47. — Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

ARTICULO 48. — Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156.

ARTICULO 49. — Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50. — Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTICULO 51. — Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

ARTICULO 52. — Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DIAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.

— REGISTRADA BAJO EL Nº 25.506 —

RAFAEL PASCUAL. — EDUARDO MENEM. — Guillermo Aramburu. — Juan C. Oyarzún.

ANEXO

Información: conocimiento adquirido acerca de algo o alguien.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;

b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;

c) la verificación de la autenticidad y la validez de los certificados involucrados.

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;

2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;

3. Ser apto para el desempeño de sus funciones específicas;

4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;

5. Cumplir con los estándares técnicos y de auditoría que establezca la Autoridad de Aplicación.

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

URUGUAY

DECRETO 382 – 17/09/03

REGLAMENTACIÓN DEL USO DE LA FIRMA DIGITAL

VISTO: lo dispuesto por los artículos 129 de la Ley 16.002 de 24 de noviembre de 1988, los artículos 694 a 697 de la Ley 16.736 de 5 de enero de 1996 y el artículo 25 de la Ley 17.243 de 29 de junio de 2000, en cuanto prevén el uso de medios informáticos y telemáticos.

RESULTANDO: Que con la sanción del artículo 25 de la Ley 17.243 se reconoce el empleo de la firma digital y su eficacia jurídica para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma confiable de las personas que realicen transacciones electrónicas.

Que asimismo, la sanción del artículo 129 de la ley 16.002 y de los artículos 694 a 697 de la ley N° 16.736 impulsa la progresiva despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso de la comunidad a la información y posibilitar la realización de trámites por Internet de forma segura.

CONSIDERANDO: Que resulta conveniente reglamentar las disposiciones legales precitadas.

ATENTO: a lo precedentemente expuesto y a lo dispuesto por el artículo 168 numeral 4° de la Constitución de la República.

EL PRESIDENTE DE LA REPÚBLICA

Actuando en Consejo de Ministros

DECRETA:

Artículo 1°: El presente decreto reglamenta el uso de la firma digital y el reconocimiento de su eficacia jurídica.

Artículo 2°: Definiciones.- A los efectos de este Decreto, se establecen las siguientes definiciones:

a) Firma Digital es el resultado de aplicar a un documento un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita, simultáneamente, identificar al firmante y detectar cualquier alteración del documento digital posterior a su flf11la.

b) Prestador de servicios de certificación es una tercera parte que expide certificados digitales, pudiendo prestar además, otros servicios relacionados con la firma digital.

c) Certificado Digital es un documento digital firmado digitalmente por un Prestador de servicios de certificación, que vincula la identidad del titular del mismo con una clave pública y su correspondiente clave privada.

d) Clave Privada es la clave generada por un proceso matemático, que contiene datos únicos que el firmante utiliza para crear la firma digital. Su conocimiento y control es exclusivo del firmante. Si el firmante decidiera compartirla, se imputará como suyo todo aquello que fuera realizado mediante el uso de la misma.

e) Clave pública es aquella clave generada por el mismo proceso matemático que genera la clave privada. Contiene datos únicos que permiten verificar la firma digital del firmante. Su conocimiento es público.

f) Lista de Certificados Revocados de un prestador de servicios de certificación es un archivo firmado digitalmente por éste, en el que constan los números de serie y fecha de revocación de todos los certificados revocados del Prestador de servicios de certificación.

g) Firmante o Signatario, es la persona física que cuenta con un Certificado Digital que utiliza para firmar digitalmente.

h) Periodo de Validez, es el período de vigencia del Certificado Digital.

Artículo 3°: Validez y eficacia de la firma digital.- La firma digital tendrá idéntica validez y eficacia a la firma autógrafa, siempre que esté debidamente autenticada por claves u otros procedimientos seguros de acuerdo a la tecnología informática que:

1. garanticen que la firma digital se corresponde con el certificado digital emitido por un prestador de servicios de certificación de firma digital, que lo asocia con la identificación del signatario;

2. aseguren que la firma digital se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado; y

3. garanticen que la firma digital ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado digital.

Articulo 4°: Valor probatorio de la firma digital.- La firma digital tendrá respecto al documento respectivo, idéntico valor probatorio al que tiene la firma manuscrita con respecto al documento consignado en papel, siempre que la misma haya sido creada mediante mecanismos de clave pública y privada u otros procedimientos acordes a la evolución de estándares tecnológicos internacionalmente reconocidos como fiables que cumplan con las exigencias establecidas en el artículo precedente. .

Artículo 5°: Requisitos del Certificado Digital.- El Certificado Digital del firmante deberá cumplir con los siguientes requisitos:

1. Contar como mínimo con la siguiente información del titular del certificado:

a. Nombre completo tal como aparece en el documento de identidad

b. Número, tipo y país emisor del documento de identidad

c. La clave pública asociada a la clave privada.

2. Número de serie.

3. Identificación del prestador de servicios de certificación.

4. Período de validez.

5. Firma Digital del prestador de servicios de certificación.

6. Debe estar vigente.

7. No debe estar revocado a la fecha de la firma.

8. Haber sido creado de acuerdo a las políticas del prestador de servicios de certificación que cumplan con lo establecido en el artículo 6.

Artículo 6°: Requisitos de emisión del Certificado Digital.- Los requisitos para la emisión de Certificados Digitales serán los siguientes:

a) Presencia física del solicitante del certificado con documento de identidad vigente y válido en la República Oriental del Uruguay.

b) Un contrato en soporte papel, con fecha de emisión, en el que se consigna la información exacta trasladada de la documentación presentada firmado en forma manuscrita en el que deberá constar:

I) Responsabilidades del Solicitante respecto de la clave Privada cuya clave pública correspondiente se consigna en el certificado y todos los usos que a la misma se le dieran.

ll) Declaración del solicitante de su total conocimiento y aceptación de la Declaración de Prácticas de Certificación y/o Política de Certificación correspondientes al certificado solicitado.

lll) Responsabilidades del solicitante y del prestador de servicios de certificación respecto a la solicitud de revocación de un certificado, consignando plazos de responsabilidad.

c) Generar la clave privada cuya clave pública correspondiente se consignará en el certificado.

Artículo 7°: Cese de actividades del prestador de servicios de certificación.- Si el prestador de servicios de certificación cesara sus actividades está obligado a comunicar dicha situación a través del Diario Oficial y cualquier otro medio que considere pertinente, a mantener o derivar el servicio de recepción de solicitudes de revocación y a actualizar y publicar la Lista de Certificados Revocados hasta que haya vencido el último de los certificados emitidos.

Artículo 8°: Actualización y publicación de la Lista de certificados Revocados.- El prestador de servicios de certificación deberá actualizar y publicar la Lista de Certificados Revocados al menos cada 24 horas.

Artículo 9°: Equivalencia de certificados.- Los certificados que expidan los prestadores de servicios de certificación establecidos en otros Estados, de acuerdo con su respectiva legislación, se considerarán equivalentes a los expedidos por los establecidos en la República, siempre que los mismos hayan sido emitidos con garantías de confiabilidad similares a las exigidas por este decreto, y que exista reciprocidad del país de origen con respecto de los certificados emitidos en el Uruguay

Artículo 10°: Comuníquese, publíquese, etc.

PERU

Ley Nº 27.269 Ley de firmas y certificados digitales.

EL PRESIDENTE DE LA REPUBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente

LEY DE FIRMAS Y CERTIFICADOS DIGITALES

Artículo l. Objeto de la ley

La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de la firma manuscrita.

Artículo 2. Ambito de aplicación

La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

Artículo 3. Firma digital

La firma digitales aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Artículo 4. Titular de la firma digital

El titular de la firma digitales la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5. Obligaciones del titular de la firma digital

El titular de la firma digital tiene la obligación de brindar a las entidades de certificación ya los terceras con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

Artículo 6. Certificado digital

El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula una parte claves con una persona determinada confirmando su identidad.

Artículo 7. Contenido del certificado digital

Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación

Artículo 8.- Confidencialidad de la información

La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los finas señalados en la presente ley.

Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9. Cancelación del certificado digital

La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital,
2. Por revocatoria de la entidad certificante o
3. Por expiración del plazo de vigencia
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10. Revocación del certificado digital

La Entidad de Certificación revocará el certificado digital en los siguientes casos:

1. Se determine que la información contenida en el certificado digital sea inexacta o haya sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de certificación.

Artículo 11. Reconocimiento del certificados emitidos por entidades extranjeras

Los Certificadas de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificadas sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propias certificados, el cumplimiento dé los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

Artículo 12. Entidad de Certificación

La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.

Artículo 13. Entidad de Registro o Verificación

La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14. Depósito de los Certificados Digitales

Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley.

El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización.

A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.

Artículo 15. Inscripción de Entidades de Certificación y de Registro o Verificación

El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.

La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales.

Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

Artículo 16. Reglamentación

DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES

PRIMERA. Mientras se cree el Registro señalado en el Artículo 150, la validez de los actos celebrados por Entidades de Certificación y Entidades de Registro o Verificación, en el ámbito de la presente ley, está condicionada a la inscripción respectiva dentro de los 45 (cuarenta y cinco) días siguientes a la creación el referido Registro.

SEGUNDA. El Reglamento de la presente ley incluirá un glosario de términos referidos a esta ley y a las firmas electrónicas en general, observando las definiciones establecidas por los organismos internacionales de los que el Perú es parte.

TERCERA. La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los ocho días del mes de mayo del dos mil.

MARTHA HILDEBRANDT PÉREZ TRE VINO
Presidenta del Congreso de la República

RICARDO MARCENARO FRERS
Primer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de mayo del año dos mil.

ALBERTO FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y
Ministro de Justicia

LEY NÚMERO 27.310

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY QUE MODIFICA EL ARTÍCULO 112 DE LA LEY NÚMERO 27.269

Objeto de la ley
Modificase el Artículo 110 de la Ley NÚMERO 27.269, el mismo que quedará redactado de la

siguiente manera:

Artículo 110.

Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiséis días del mes de junio del dos mil.

CHILE

Ley 19799

Ley sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma

TÍTULO I. DISPOSICIONES GENERALES

Artículo 1º.- La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso. Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel. Toda interpretación de los preceptos de esta ley deberá guardar armonía con los principios señalados.

Artículo 2º.- Para los efectos de esta ley se entenderá por:

a) Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

b) Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;

c) Certificador o Prestador de Servicios de Certificación: entidad prestadora de servicios de certificación de firmas electrónicas;

d) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior;

e) Entidad Acreditadora: la Subsecretaría de Economía, Fomento y Reconstrucción;

f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;

g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría, y

h) Usuario o titular: persona que utiliza bajo su exclusivo control un certificado de firma electrónica.

Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando

constan por escrito. Lo dispuesto en el inciso anterior no será aplicable a los actos y contratos otorgados o celebrados en los casos siguientes:

a) Aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;

b) Aquellos en que la ley requiera la concurrencia personal de alguna de las partes; y,

c) Aquellos relativos al derecho de familia. La firma electrónica, cualquiera sea su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en el artículo siguiente.

Artículo 4º.- Los documentos electrónicos que tengan la calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada.

Artículo 5°.- Los documentos electrónicos podrán presentarse en juicio y, en el evento de que sean usados como medio de prueba, habrán de seguirse las reglas siguientes:

1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales; y

2.- Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el numeral anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.

TITULO II. USO DE FIRMAS ELECTRÓNICAS POR LOS ÓRGANOS DEL ESTADO

Artículo 6º.- Los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica. Se exceptúan aquellas actuaciones para las cuales la Constitución Política o la ley exija una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, o requiera la concurrencia personal de la autoridad o funcionario que deba intervenir en ellas. Lo dispuesto en este título no se aplicará a las empresas públicas creadas por ley, las que se regirán por las normas previstas para la emisión de documentos y firmas electrónicas por particulares.

Artículo 7º.- Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel. Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada.

Artículo 8º.- La personas podrán relacionarse con los órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten al procedimiento descrito por la ley y que tales técnicas y medios sean compatibles con los que utilicen dichos órganos. Los órganos del Estado deberán evitar, al hacer uso de firmas electrónicas, que se restrinja injustificadamente el acceso a las prestaciones que brinden y a la publicidad y transparencia que rijan sus actuaciones y, en general, que se cause discriminaciones arbitrarias.

Artículo 9º.- La certificación de las firmas electrónicas avanzadas de las autoridades o funcionarios de los órganos del Estado se realizará por los respectivos ministros de fe. Si éste no se encontrare establecido en la ley, el reglamento a que se refiere el artículo 10 indicará la forma en que se designará un funcionario para estos efectos. Dicha certificación deberá contener, además de las menciones que corresponda, la fecha y hora de la emisión del

documento .Los efectos probatorios de la certificación practicada por el ministro de fe competente serán equivalentes a los de la certificación realizadas por un prestador acreditado de servicios de certificación. Sin perjuicio de lo dispuesto en el inciso primero, los órganos del Estado podrán contratar los servicios de certificación de firmas electrónicas con entidades certificadoras acreditadas, si ello resultare más conveniente, técnica o económicamente, en las condiciones que señale el respectivo reglamento.

Artículo 10.- Los reglamentos aplicables a los correspondientes órganos del Estado regularán la forma cómo se garantizará la publicidad, seguridad, integridad y eficacia en el uso de las firmas electrónicas, y las demás necesarias para la aplicación de las normas de este Título.".

TITULO III. DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 11.- Son prestadores de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar. Asimismo, son prestadores acreditados de servicios de certificación las personas jurídicas nacionales o extranjeras, públicas o privadas, domiciliadas en Chile y acreditadas en conformidad al Título V de esta ley, que otorguen certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Artículo 12.- Son obligaciones del prestador de servicios de certificación de firma electrónica:

a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano;

b) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada;

c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;

d) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

e) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;

f) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos, y

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores y Nº 19.628, sobre Protección de la Vida Privada.

Artículo 13.- El cumplimiento, por parte de los prestadores no acreditados de servicios de certificación de firma electrónica, de las obligaciones señaladas en las letras a), b), c) y j) del artículo anterior, será considerado por el juez como un antecedente para determinar si existió la debida diligencia, para los efectos previstos en el inciso primero del artículo siguiente

Artículo 14. Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia. Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica. Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquéllos homologados en virtud de lo dispuesto en el inciso final del artículo 15.El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero. El proveedor de servicios de certificación quedará eximido de responsabilidad por los daños y perjuicios causados por el uso que exceda de los límites indicados en el certificado. En ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.

TÍTULO IV. DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Artículo 15.- Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:

a) Un código de identificación único del certificado;

b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;

c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y

d) Su plazo de vigencia. Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente.

Artículo 16.- Los certificados de firma electrónica quedarán sin efecto, en los siguientes casos:

1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;

2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:

a) A solicitud del titular del certificado;

b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;

c) Por resolución judicial ejecutoriada, o

d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 24;

3) Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados que señala el artículo 18, en razón de lo dispuesto en el artículo 19 o del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) y h) del artículo 12; y,

4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 12.La revocación de un certificado en las circunstancias de la letra d) del número 2) de este artículo, así como la suspensión cuando ocurriere por causas técnicas, será comunicada previamente por el prestador al titular del certificado, indicando la causa y el momento en que se hará efectiva la revocación o la suspensión. En cualquier caso, ni la revocación ni la suspensión privarán de valor a los certificados antes del momento exacto en que sean verificadas por el prestador. El término de vigencia de un certificado de firma electrónica por alguna de las causales señaladas precedentemente será inoponible a terceros mientras no sea eliminado del registro de acceso público.

TITULO V. DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Artículo 17.-La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en esta ley y en el reglamento, permitiendo su inscripción en el registro que se señala en el artículo 18. Para ser acreditado, el prestador de servicios de certificación deberá cumplir, al menos, con las siguientes condiciones:

a) Demostrar la fiabilidad necesaria de sus servicios;

b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;

c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;

d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;

e) Haber contratado un seguro apropiado en los términos que señala el artículo 14; y,

f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

Artículo 18.- El procedimiento de acreditación se iniciará mediante solicitud ante la Entidad Acreditadora, a la que se deberá acompañar los antecedentes relativos a los requisitos del artículo 17 que señale el reglamento y el comprobante de pago de los costos de la acreditación. La Entidad Acreditadora deberá resolver fundadamente sobre la solicitud en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse. Si el interesado denunciare el incumplimiento de ese plazo ante la propia autoridad y ésta no se pronunciare dentro del mes siguiente, la solicitud se entenderá aceptada. La Entidad Acreditadora podrá contratar expertos con el fin de verificar el cumplimiento de los requisitos señalados en el artículo 17. Otorgada la acreditación, el prestador será inscrito en un registro público que a tal efecto llevará la Entidad Acreditadora, al que se podrá acceder por medios electrónicos. Durante la vigencia de su inscripción en el registro, el prestador acreditado deberá informar a la Entidad Acreditadora cualquier modificación de las condiciones que permitieron su acreditación.

Artículo 19 .- Mediante resolución fundada de la Entidad Acreditadora se podrá dejar sin efecto la acreditación y cancelar la inscripción en el registro señalado en el artículo 18, por alguna de las siguientes causas:

a) Solicitud del prestador acreditado;

b) Pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o peritos que la Entidad Acreditadora ocupe en la inspección a que se refiere el artículo 20; y,

c) Incumplimiento grave o reiterado de las obligaciones que establece esta ley y su reglamento.

En los casos de las letras b) y c), la resolución será adoptada previa audiencia del afectado y se podrá reclamar de ella ante el Ministro de Economía, Fomento y Reconstrucción, dentro del plazo de cinco días contados desde su notificación. El Ministro tendrá un plazo de treinta días para resolver. Dentro de los diez días siguientes a la fecha en que se notifique la resolución que éste dicte o, en su caso, desde que se certifique que la reclamación administrativa no fue resuelta dentro de plazo, el interesado podrá interponer reclamación jurisdiccional, para ante la Corte de Apelaciones de su domicilio. La reclamación deberá ser fundada y para su agregación a la tabla, vista y fallo, se regirá por las normas aplicables al recurso de protección. La resolución de la Corte de Apelaciones no será susceptible de recurso alguno. Los certificadores cuya inscripción haya sido cancelada, deberán comunicar inmediatamente este hecho a los titulares de firmas electrónicas certificadas por ellos. Sin perjuicio de ello, la Entidad Acreditadora publicará un aviso dando cuenta de la cancelación, a costa del certificador. A partir de la fecha de esta publicación, quedarán sin efecto los certificados, a menos que los datos de los titulares sean transferidos a otro certificador acreditado, en conformidad con lo dispuesto en la letra h) del artículo 12. Los perjuicios que pueda causar la cancelación de la inscripción del certificador para los titulares de los certificados que se encontraban vigentes hasta la cancelación, serán de responsabilidad del prestador.

Artículo 20.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Entidad Acreditadora ejercerá la facultad inspectora sobre los mismos y podrá, a tal efecto, requerir información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados, de conformidad al reglamento.

Artículo 21.- La Entidad Acreditadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los certificadores acreditados.

Artículo 22.- Los recursos que perciba la Entidad Acreditadora por parte de los prestadores acreditados de servicios de certificación constituirán ingresos propios de dicha entidad y se incorporarán a su presupuesto.

TITULO VI. DERECHOS Y OBLIGACIONES DE LOS USUARIOS DE FIRMAS ELECTRÓNICAS

Artículo 23.- Los usuarios o titulares de firmas electrónicas tendrán los siguientes derechos:

1°. A ser informado por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que éstos se comprometan a seguir en la prestación del servicio, previamente a que se empiece a efectuar;

2°.A la confidencialidad en la información proporcionada a los prestadores de servicios de certificación. Para ello, éstos deberán emplear los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos;

3°. A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se convinieren;

4°. A que el prestador de servicios o quien homologue sus certificados le proporcionen la información sobre sus domicilios en Chile y sobre todos los medios a los que el usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;

5°. A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 4) del artículo 16 de la presente ley, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

6°. A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 3) del artículo 16 de la presente ley, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador;

7°. A traspasar sus datos a otro prestador de servicios de certificación;

8º. A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;

9º. A acceder, por medios electrónicos, al registro de prestadores acreditados que mantendrá la Entidad Acreditadora, y

10º. A ser indemnizado y hacer valer los seguros comprometidos, en conformidad con el artículo 15 de la presente ley.

Los usuarios gozarán de estos derechos, sin perjuicio de aquellos que deriven de la Ley Nº 19.628, sobre Protección de la Vida Privada y de la Ley Nº 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10° de este artículo, ejercerlos conforme al procedimiento establecido en esa última normativa.

Artículo 24.- Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

TITULO VII. REGLAMENTOS

Artículo 25.- El Presidente de la República reglamentará esta ley en el plazo de noventa días contados desde su publicación, mediante uno o más decretos supremos del Ministerio de Economía, Fomento y Reconstrucción, suscritos también por los Ministros de Transportes y Telecomunicaciones y Secretario General de la Presidencia. Lo anterior es sin perjuicio de los demás reglamentos que corresponda aprobar, para dar cumplimiento a lo previsto en el artículo 10.

Artículo transitorio.- El mayor gasto que irrogue a la Subsecretaría de Economía, Fomento y Reconstrucción las funciones que le asigna esta ley, durante el año 2002, se financiará con los recursos consultados en su presupuesto.

ESPAÑA

Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. (B.O.E. 18.09.1999)

En la sesión del Consejo de Ministros de Telecomunicaciones de la Unión Europea, celebrada el 22 de abril de 1999, se ha informado favorablemente la adopción de una posición común, respecto del proyecto de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica.

El Estado español ha tenido una participación activa en el logro de la posición común que facilita la tramitación del texto, al recoger éste los elementos suficientes para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica. En ese sentido, existen ya en España diversas normas sobre la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas por medios telemáticos, dictadas por la Administración tributaria. La Comisión Nacional del Mercado de Valores, por su parte, ha aprobado y puesto en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas. Asimismo, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, anuncia 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, 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 Telégrafos.

En el proyecto de Directiva se incorpora, a solicitud del Estado español, una novedad, recogida en el apartado c) del anexo II, entre los requisitos exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos. Esta novedad consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante.

Existe, además, en España un sector empresarial que podría prestar un servicio de certificación de la firma electrónica con suficiente calidad. Se considera que debe introducirse, cuanto antes, la disciplina que permita utilizar, con la adecuada seguridad jurídica, este medio tecnológico que contribuye al desarrollo de lo que se ha venido en denominar, en la Unión Europea, la sociedad de la información, La urgencia de la aprobación de esta norma deriva, también, del deseo de dar, a los usuarios de los nuevos servicios, elementos de confianza en los sistemas, permitiendo su introducción y rápida difusión.

Por ello, este Real Decreto-ley persigue, respetando el contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación. De igual modo, este Real Decreto-ley determina el registro en el que habrán de inscribirse los prestadores de servicios de certificación y el régimen de inspección administrativa de su actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento.

La presente disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio.

En su virtud, a propuesta del Ministro de Fomento, de la Ministra de Justicia y del Ministro de Industria y Energía, previo informe del Consejo General del Poder Judicial y de la Agencia de Protección de Datos, tras la deliberación del Consejo de Ministros, en su reunión celebrada el día 17 de septiembre de 1999, y en uso de la autorización concedida en el artículo 86 de la Constitución,

DISPONGO:

TÍTULO I . Disposiciones generales

CAPÍTULO ÚNICO . Disposiciones generales

Artículo 1. Ámbito de aplicación.

1. Este Real Decreto-ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

Artículo 2. Definiciones.

A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:

a) «Firma electrónica»: Es 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.

b) «Firma electrónica avanzada»: 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 detestable cualquier modificación ulterior de éstos.

c) «Signatario»: Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

d) «Datos de creación de firma»: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica.

e) «Dispositivo de creación de firma»: Es un programa o un aparato informático que sirve para aplicar los datos de creación de firma.

f) «Dispositivo seguro de creación de firma»: Es un dispositivo de creación de firma que cumple los requisitos establecidos en el artículo 19.

g) «Datos de verificación de firma»: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

h) «Dispositivo de verificación de firma»: Es un programa o un aparato informático que sirve para aplicar los datos de verificación de firma.

i) «Certificado»: Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

j) «Certificado reconocido»: Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

k) «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.

l) «Producto de firma electrónicas: Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

ll) «Acreditación voluntaria del prestador de servicios de certificación»: Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

Artículo 3. Efectos jurídicos de la firma electrónica.

1. 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.

2. A la firmar electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

TÍTULO II . La prestación de servicios de certificación

CAPITULO I .Principios generales

Artículo 4. Régimen de libre competencia.

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea.

2. La prestación de los servicios de certificación por las Administraciones o los organismos o sociedades de ellas dependientes se realizará con la debida separación de cuentas y con arreglo a los principios de objetividad, transparencia y no discriminación.

Artículo 5. Empleo de la firma electrónica por las Administraciones públicas.

a) Se podrá supeditar por la normativa estatal o, en su caso, autonómica el uso de la firma electrónica en el seno de las Administraciones públicas y sus entes públicos y en las relaciones que con cualesquiera de ellos mantengan los particulares, a las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento.

Las condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora. respecto de los documentos electrónicos integrados en un expediente administrativo. El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica a las que se refiere este apartado sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y se dictarán a propuesta del Ministerio de Administraciones Públicas y previo informe del Consejo Superior de Informática.

b) Las condiciones adicionales a las que se refiere el apartado anterior 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, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o extranjeras.

3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarios, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

Artículo 6. Sistemas de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica.

1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios.

2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 1 1/1 998, de 24 de abril, General de Telecomunicaciones; en la Ley 21/1992, de 16 de julio, de Industria, y en la demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1 establecerá las condiciones que permitan coordinar los sistemas de certificación.

3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan

voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen.

4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que se haya pedido certificación. También tomarán en cuenta el cumplimiento, por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado.

5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

Artículo 7. Registro de Prestadores de Servicios de Certificación.

1. Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España. Su regulación se desarrollará por Real Decreto.

2. La solicitud de inscripción habrá de formularse, aportando la documentación que se establezca reglamentariamente, a efectos de la identificación del prestador de servicios de certificación y de justificar que éste reúne los requisitos necesarios, en cada caso, para ejercer su actividad. También será objeto de inscripción ulterior cualquier circunstancia relevante, a efectos de este Real Decreto-ley, relativa al prestador de servicios de certificación, como su acreditación o estar en condiciones de expedir certificados reconocidos.

La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente.

3. El Registro de Prestadores de Servicios de Certificación será público y deberá mantener permanentemente actualizada y a disposición de cualquier persona una relación de los inscritos, en la que figurarán su nombre o razón social, la dirección de su página en Internet o de correo electrónico, los datos de verificación de su firma electrónica y, en su caso, su condición de acreditado o de tener la posibilidad de expedir certificados reconocidos. En la citada relación figurarán, también, cualesquiera otros datos complementarios que se determinen por Real Decreto.

Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral. El suministro de esta información podrá sujetarse al pago de una tasa, cuyos elementos esenciales se determinarán por ley.

CAPÍTULO II .Certificados

Artículo 8- Requisitos para la existencia de un certificado reconocido.

1. Los certificados reconocidos, definidos en el artículo 2.j) de este Real Decreto-ley, tendrán el siguiente contenido:

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, 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.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) 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.

f) 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.

g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario

h) El comienzo y el fin del período de validez del certificado.

i) Los límites de uso del certificado, si se prevén.

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

2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Artículo 9. Vigencia de los certificados.

1. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:

a) Expiración del período de validez del certificado. Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.

c) Pérdida o inutilización por daños del soporte del certificado.

d) Utilización indebida por un tercero.

e) Resolución judicial o administrativa que lo ordene-

f) 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.

g) 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.

h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

2. La pérdida de eficacia de los certificados, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado surtirá efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11.e).

3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y 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 la prueba de que los terceros conocían las circunstancias invalidantes del certificado.

4. 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. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores.

Artículo 10. Equivalencia de certificados.

Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste, expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España. siempre que se cumplan alguna de las siguientes condiciones:

a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.

b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.

c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPÍTULO III. Condiciones exigibles a los prestadores de servicios de certificación

Artículo 11. Obligaciones de los prestadores de servicios de certificación.

Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

a) 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 esta 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 aquellos.

b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.

c) 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.

d) 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.

e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o perdida 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.

f) 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, 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.

g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.

h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

Artículo 12. Obligaciones exigibles a los prestadores de servicios de certificación que expidan certificados reconocidos.

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:

a) Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

b) Demostrar la fiabilidad necesaria de sus servicios.

c) Garantizar la rapidez y la seguridad en la prestación del 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.

d) 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.

e) 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.

f) 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.

g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus

servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.

Inicialmente, la garantía cubrirá, al menos, 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. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.

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 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.

h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.

i) 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 quien lo solicite. Para comunicar esta información podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.

j) Utilizar sistemas fiables para almacenar certificados, de modo tal que:

1). Sólo personas autorizadas puedan consultarlos, 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,

k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

Artículo 13. Cese de la actividad.

1. El prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo 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. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

2. 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 indicada en el anterior apartado, el cese de su actividad, y el destino que vaya a dar a los certificados especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto. Igualmente, indicará cualquier otra circunstancia relevante, que pueda impedir la continuación de su

actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de un procedimiento de quiebra o suspensión de pagos respecto de él.

3. La inscripción del prestados de servicios de certificación en el Registro de Prestadores de Servicios de Certificación será cancelada, de oficio, por el Ministerio de Justicia, cuando aquél cese en su actividad. El Ministerio de Justicia se hará cargo de la información relativa a los certificados que se hubieren dejado sin efecto por el prestador de servicios de certificación, a efectos de lo previsto en el artículo 12.h).

Artículo 14. Responsabilidad de los prestadores de servicios de certificación.

1). Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

2). El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

3). La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.

4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Artículo 15. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación al que se refiere este Real Decreta-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad le los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre. Ello se entiende sin perjuicio de lo que, en la legislación

específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

En todo caso, se estará a lo previsto en las normas sobre protección de datos indicadas en el apartado 1 de este artículo.

CAPÍTULO IV . Inspección y control de la actividad de los prestadores de servicios de certificación

Artículo 16. Supervisión y control.

1. 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 este Real Decreto-ley 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.

2. 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.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, de lo dispuesto en el artículo 11.c), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Esta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador, con arreglo a la legislación que regula su actividad.

Artículo 17. Deber de colaboración.

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 conciernan al prestador de servicios.

Artículo 18. Resoluciones del órgano de supervisión.

La Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan este Real Decreto-ley y sus disposiciones de desarrollo.

TÍTULO III. Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

CAPÍTULO ÚNICO. Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable

Artículo 19. Dispositivos seguros de creación de firma electrónica.

A efectos del artículo 2.f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:

1.º. Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2.º. Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3.º. Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4.º. 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.

Artículo 20. Normas técnicas.

1. Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el «Diario Oficial de las Comunidades Europeas» son conformes con lo previsto en la letra e) del artículo 12 y en el artículo 19.

2. Sin perjuicio de esta presunción, los números de referencia de esas normas se publicarán en el «Boletín Oficial del Estado».

Artículo 2l. Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica.

1. Los órganos de certificación a los que se refiere el artículo 6 podrán certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de evaluación acreditadas.

En la evaluación del cumplimiento de los requisitos previstos en el artículo 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el articulo anterior u otras que determinen los órganos de acreditación y de certificación, y cuyas referencias se publiquen en el «Boletín Oficial del Estado».

2. Se reconocerá eficacia a los certificados sobre dispositivos seguros de creación de firma que hayan sido expedidos por los organismos designados para ello por los Estados miembros de la Unión Europea, cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.

Artículo 22. Dispositivos de verificación de firma.

1. Los dispositivos de verificación de firma electrónica avanzada deben garantizar lo siguiente:

a) Que la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente.

b) Que el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

c) Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo,

d) Que se verifica de forma fiable el certificado.

e) Que puede detectarse cualquier cambio relativo su seguridad.

2. El Real Decreto al que se refiere el artículo 6 podrá establecer los términos en los que las entidades de evaluación y los órganos de certificación podrán evaluar y certificar, respectivamente, el cumplimiento, por los dispositivos de verificación de firma electrónica avanzada, de los requisitos establecidos en este artículo.

TÍTULO IV. Tasa por el reconocimiento de acreditaciones y certificaciones

CAPÍTULO ÚNICO. Tasa por el reconocimiento de acreditaciones y certificaciones

Artículo 23. Régimen aplicable a la tasa.

1. La gestión precisa para el reconocimiento de las acreditaciones y de las certificaciones con arreglo a los artículos 6, 21 y 22, por los órganos públicos competentes, se grava con una tasa, a la que se aplicará el siguiente régimen:

a) Constituye el hecho imponible el reconocimiento dichos órganos de la acreditación de los prestadores de servicios o de la certificación de los dispositivos de creación o de verificación de firma a que se refieren los artículos 6, 21 y 22.

b) Es sujeto pasivo la persona natural o jurídica que se beneficie del reconocimiento de la correspondiente acreditación o certificación.

c) Su cuota es de 47.500 pesetas (285,48 euros) por cada acreditación o certificación reconocida. Esta cantidad podrá ser actualizada por Real Decreto.

d) Se devengará cuando se presente la solicitud de reconocimiento de la correspondiente acreditación o certificación.

2. La forma de liquidación de la tasa se establecerá reglamentariamente.

TÍTULO V. Infracciones y sanciones

CAPÍTULO ÚNICO. Infracciones y sanciones

Artículo 24. Clasificación de las infracciones.

Las infracciones de las normas reguladores de la firma electrónica y los servicios de certificación se clasifican en muy graves, graves y leves.

Artículo 25. Infracciones.

1. Son infracciones muy graves:

a) 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).

b) 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 articulo 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.

c) 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 a este Real Decreto-ley.

2. Son infracciones graves:

a) 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.

b) 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.

c) 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, cuando no concurran las circunstancias previstas en el apartado 1.b) de este artículo.

d) La falta de comunicación por el prestados de servicios de certificación al Ministerio de Justicia, en los plazos previstos en el artículo 13, del cese de su actividad o de la iniciación, respecto de él, de un procedimiento de suspensión de pagos o de quiebra.

e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarlo a cabo, con arreglo a este Real Decreto-ley.

f) El incumplimiento de las resoluciones dictadas por la Secretaría General de Comunicaciones para asegurar que el prestador de servicios de certificación se ajuste a este Real Decreto-ley, cuando no deba considerarse como infracción muy grave, conforme al apartado 1.c) de este artículo.

3. Son infracciones leves:

a) 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, excepto la c), cuando no deba considerarse como infracción grave, de acuerdo con lo previsto en el apartado 2.a) de este artículo.

b) La expedición de certificados reconocidos que incumplan alguno de los requisitos establecidos en el artículo 8.

c) 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 de este Real Decreto-ley por los prestadores de servicios de certificación.

d) Cualquier otro incumplimiento de las obligaciones impuestas a los prestadores de servicios de certificación por este Real Decreto-ley, salvo el de la recogida en el artículo 11.c) o que deba ser considerado como infracción grave o muy grave, de acuerdo con lo dispuesto en los apartados anteriores.

Artículo 26. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, 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 resultara 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 100.000.000 de pesetas (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 sus 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 al Registro de Prestadores de Servicios de Certificación para que cancele la inscripción del prestador de servicios sancionado.

b) 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 resultara 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 a, 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 50.000.000 de pesetas (300.506,04 euros).

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 euros).

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación de la resolución sancionadora en el «Boletín Oficial del Estado» y en dos periódicos de difusión nacional, una vez que aquélla tenga carácter firme.

3. La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992. lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El daño causado, siempre que no haya sido tomado en consideración para calificar la infracción como leve, grave o muy grave.

d) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

4. Se anotarán en el Registro de Prestadores de Servicios de Certificación las sanciones impuestas por resolución firme a éstos por la comisión de cualquier infracción grave o muy grave. Las notas relativas a las sanciones se cancelarán una vez transcurridos los plazos de prescripción de las sanciones administrativas previstos en la Ley reguladora del procedimiento administrativo común.

5. Las cuantías señaladas en este artículo serán actualizadas periódicamente por el Gobierno, mediante Real Decreto, teniendo en cuenta la variación de los índices de precios al consumo.

Artículo 27. Medidas cautelares.

En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte. Estas medidas podrán 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. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

Artículo 28. Procedimiento sancionador.

1. El ejercicio de la potestad sancionadora atribuida por este Real Decreto-ley corresponde a la Secretaría General de Comunicaciones del Ministerio de Fomento. Para ello, la Secretaría General de Comunicaciones se sujetará al procedimiento aplicable, con carácter general, al ejercicio de la potestad sancionadora por las Administraciones públicas.

2. El Ministerio de Justicia y los demás órganos que ejercen competencias con arreglo a este Real Decreto-ley y sus normas de desarrollo podrán instar la incoación de un procedimiento sancionador, mediante petición razonada dirigida a la Secretaría General de Comunicaciones

Disposición adicional única. Posibilidad de emisión por las entidades públicas de radiodifusión de una Comunidad Autónoma en el territorio de otras con las que aquélla tenga espacios radioeléctricos colindantes.

Las entidades autonómicas habilitadas, con arreglo a la Ley, para prestar el servicio de radiodifusión digital terrenal, podrán emitir en el territorio de otras Comunidades Autónomas con las que aquélla tenga espacios radioeléctricos colindantes. Para ello, será preciso que exista acuerdo entre las Comunidades Autónomas afectadas y que, en cada territorio, se empleen los bloques de frecuencias planificados en el Plan Técnico Nacional de Radiodifusión Sonora Digital Terrenal, para el ámbito autonómico.

Disposición transitoria única. Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de este Real Decreto-ley.

Los prestadores de servicios de certificación ya establecidos en España y cuya actividad se rija por una normativa específica habrán de adaptarse a este Real Decreto-ley en el plazo de un año desde su entrada en vigor. No obstante conservarán su validez los certificados ya expedidos que hayan surtido efectos.

Disposición final primera. Fundamento constitucional.

Este Real Decreto-ley se dicta al amparo del artículo 149.1.8ª, 18ª y 21ª de la Constitución, que atribuye competencia exclusiva al Estado en materia de legislación civil, de bases del régimen jurídico de las Administraciones Públicas y de telecomunicaciones.

Disposición final segunda. Habilitación al Gobierno.

Se habilita al Gobierno para desarrollar, mediante Reglamento, lo previsto en este Real Decreto.

Disposición final tercera. Entrada en vigor.

El presente Real Decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid a 17 de septiembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno. JOSÉ MARÍA AZNAR LÓPEZ

COLOMBIA

LEY 527 DE 1999

El Congreso de Colombia

DECRETA:

PARTE I

PARTE GENERAL

CAPITULO I

Disposiciones generales

Artículo 1°. *Ambito de aplicación*. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Artículo 2°. *Definiciones*. Para los efectos de la presente ley se entenderá por:

a) **Mensaje de datos.** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

b) **Comercio electrónico.** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

c) **Firma digital.** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

d) **Entidad de Certificación.** Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

e) **Intercambio Electrónico de Datos (EDI).** La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;

f) **Sistema de Información.** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3°. *Interpretación.* En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

Artículo 4°. *Modificación mediante acuerdo.* Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

Artículo 5°. *Reconocimiento jurídico de los mensajes de datos.* No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

CAPITULO II

Aplicación de los requisitos jurídicos de los mensajes de datos

Artículo 6°. *Escrito.* Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Artículo 7°. *Firma.* Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;

b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.

Artículo 8°. *Original.* Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:

a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

Artículo 9°. *Integridad de un mensaje de datos*. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 10. *Admisibilidad y fuerza probatoria de los mensajes de datos*. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

Artículo 11. *Criterio para valorar probatoriamente un mensaje de datos*. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 12. *Conservación de los mensajes de datos y documentos*. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y

3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.

Los libros y papeles del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta.

Artículo 13. *Conservación de mensajes de datos y archivo de documentos a través de terceros*. El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

CAPITULO III

Comunicación de los mensajes de datos

Artículo 14. *Formación y validez de los contratos*. En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Artículo 15. *Reconocimiento de los mensajes de datos por las partes*. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos.

Artículo 16. *Atribución de un mensaje de datos*. Se entenderá que un mensaje de datos proviene del iniciador, cuando éste ha sido enviado por:

1. El propio iniciador.

2. Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje, o

3. Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 17. *Presunción del origen de un mensaje de datos*. Se presume que un mensaje de datos ha sido enviado por el iniciador, cuando:

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, para establecer que el mensaje de datos provenía efectivamente de éste, o

2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

Artículo 18. *Concordancia del mensaje de datos enviado con el mensaje de datos recibido*. Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, este último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

El destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a un error en el mensaje de datos recibido.

Artículo 19. *Mensajes de datos duplicados*. Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

Artículo 20. *Acuse de recibo*. Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del destinatario, automatizada o no, o

b) Todo acto del destinatario que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

Artículo 21. *Presunción de recepción de un mensaje de datos*. Cuando el iniciador recepcione acuse recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.

Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recepcionado cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

Artículo 22. *Efectos jurídicos*. Los artículos 20 y 21 únicamente rigen los efectos relacionados con el acuse de recibo. Las consecuencias jurídicas del mensaje de datos se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos.

Artículo 23. *Tiempo del envío de un mensaje de datos*. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.

Artículo 24. *Tiempo de la recepción de un mensaje de datos*. De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue:

a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar:

1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o

2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

Artículo 25. *Lugar del envío y recepción del mensaje de datos*. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:

a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;

b) Si el iniciador o el destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

PARTE II

COMERCIO ELECTRONICO EN MATERIA DE TRANSPORTE DE MERCANCIAS

Artículo 26. *Actos relacionados con los contratos de transporte de mercancías*. Sin perjuicio de lo dispuesto en la parte I de la presente ley, este capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea taxativa:

a) I. Indicación de las marcas, el número, la cantidad o el peso de las mercancías.

II. Declaración de la naturaleza o valor de las mercancías.

III. Emisión de un recibo por las mercancías.

IV. Confirmación de haberse completado el embarque de las mercancías;

b) I. Notificación a alguna persona de las cláusulas y condiciones del contrato.

II. Comunicación de instrucciones al transportador;

c) I. Reclamación de la entrega de las mercancías.

II. Autorización para proceder a la entrega de las mercancías.

III. Notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

d) Cualquier otra notificación o declaración relativas al cumplimiento del contrato;

e) Promesa de hacer entrega de las mercancías a la persona designada o a una persona autorizada para reclamar esa entrega;

f) Concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías;

g) Adquisición o transferencia de derechos y obligaciones con arreglo al contrato.

Artículo 27. *Documentos de transporte*. Con sujeción a lo dispuesto en el inciso 3° del presente artículo, en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 26 se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

El inciso anterior será aplicable, tanto si el requisito en él previsto está expresado en forma de obligación o si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento emitido en papel.

Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío o utilización de un documento emitido en papel, ese requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método confiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

Para los fines del inciso tercero, el nivel de confiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 26, no será válido ningún documento emitido en papel para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos emitidos en papel. Todo documento con soporte en papel que se emita en esas circunstancias deberá contener una declaración en tal sentido. La sustitución de mensajes de datos por documentos emitidos en papel no afectará los derechos ni las obligaciones de las partes.

Cuando se aplique obligatoriamente una norma jurídica a un contrato de transporte de mercancías que esté consignado, o del que se haya dejado constancia en un documento emitido en papel, esa norma no dejará de aplicarse, a dicho contrato de transporte de mercancías del que se haya dejado constancia en uno o más mensajes de datos por razón de que el contrato conste en ese mensaje o esos mensajes de datos en lugar de constar en documentos emitidos en papel.

PARTE III

FIRMAS DIGITALES, CERTIFICADOS Y ENTIDADES DE CERTIFICACION

CAPITULO I

Firmas digitales

Artículo 28. *Atributos jurídicos de una firma digital*. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.

2. Es susceptible de ser verificada.

3. Está bajo el control exclusivo de la persona que la usa.

4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.

5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

CAPITULO II

Entidades de certificación

Artículo 29. *Características y requerimientos de las entidades de certificación*. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación;

b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley;

c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

Artículo 30. *Actividades de las entidades de certificación*. Las entidades de certificación autorizadas por la Superintendencia de Industria y Comercio para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

1. Emitir certificados en relación con las firmas digitales de personas naturales o jurídicas.

2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.

3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la presente ley.

4. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

6. Ofrecer los servicios de archivo y conservación de mensajes de datos.

Artículo 31. *Remuneración por la prestación de servicios*. La remuneración por los servicios de las entidades de certificación serán establecidos libremente por éstas.

Artículo 32. *Deberes de las entidades de certificación*. Las entidades de certificación tendrán, entre otros, los siguientes deberes:

a) Emitir certificados conforme a lo solicitado o acordado con el suscriptor;

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;

c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;

d) Garantizar la prestación permanente del servicio de entidad de certificación;

e) Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores;

f) Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley;

g) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;

h) Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio;

i) Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio;

j) Llevar un registro de los certificados.

Artículo 33. *Terminación unilateral*. Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de noventa (90) días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación dando un preaviso no inferior a treinta (30) días.

Artículo 34. *Cesación de actividades por parte de las entidades de certificación.* Las entidades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte de la Superintendencia de Industria y Comercio.

CAPITULO III

Certificados

Artículo 35. *Contenido de los certificados*. Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.

2. Identificación del suscriptor nombrado en el certificado.

3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.

4. La clave pública del usuario.

5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.

6. El número de serie del certificado.

7. Fecha de emisión y expiración del certificado.

Artículo 36. *Aceptación de un certificado*. Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha guardado en un repositorio.

Artículo 37. *Revocación de certificados*. El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

1. Por pérdida de la clave privada.

2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

Una entidad de certificación revocará un certificado emitido por las siguientes razones:

1. A petición del suscriptor o un tercero en su nombre y representación.

2. Por muerte del suscriptor.

3. Por liquidación del suscriptor en el caso de las personas jurídicas.

4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.

5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.

6. Por el cese de actividades de la entidad de certificación, y

7. Por orden judicial o de entidad administrativa competente.

Artículo 38. *Término de conservación de los registros*. Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

CAPITULO IV

Suscriptores de firmas digitales

Artículo 39. *Deberes de los suscriptores*. Son deberes de los suscriptores:

1. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.

2. Suministrar la información que requiera la entidad de certificación.

3. Mantener el control de la firma digital.

4. Solicitar oportunamente la revocación de los certificados.

Artículo 40. *Responsabilidad de los suscriptores*. Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.

CAPITULO V

Superintendencia de Industria y Comercio

Artículo 41. *Funciones de la Superintendencia*. La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones:

1. Autorizar la actividad de las entidades de certificación en el territorio nacional.

2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación.

3. Realizar visitas de auditoría a las entidades de certificación.

4. Revocar o suspender la autorización para operar como entidad de certificación.

5. Solicitar la información pertinente para el ejercicio de sus funciones.

6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.

8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.

9. Emitir certificados en relación con las firmas digitales de las entidades de certificación.

10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación.

11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

Artículo 42. *Sanciones*. La Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación:

1. Amonestación.

2. Multas institucionales hasta por el equivalente a dos mil (2.000) salarios mínimos legales mensuales vigentes, y personales a los administradores y representantes legales de las entidades de certificación, hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado conductas violatorias de la ley.

3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora.

4. Prohibir a la entidad de certificación infractora prestar directa o indirectamente los servicios de entidad de certificación hasta por el término de cinco (5) años.

5. Revocar definitivamente la autorización para operar como entidad de certificación.

CAPITULO VI

Disposiciones varias

Artículo 43. *Certificaciones recíprocas*. Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Artículo 44. *Incorporación por remisión*. Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes y conforme a la ley, esos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

PARTE IV

REGLAMENTACION Y VIGENCIA

Artículo 45. La Superintendencia de Industria y Comercio contará con un término adicional de doce (12) meses, contados a partir de la publicación de la presente ley, para organizar y asignar a una de sus dependencias la función de inspección, control y vigilancia de las actividades realizadas por las entidades de certificación, sin perjuicio de que el Gobierno Nacional cree una unidad especializada dentro de ella para tal efecto.

Artículo 46. *Prevalencia de las leyes de protección al consumidor*. La presente ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor.

Artículo 47. *Vigencia y derogatoria*. La presente ley rige desde la fecha de su publicación y deroga las disposiciones que le sean contrarias.

El Presidente del honorable Senado de la República,

Fabio Valencia Cossio.

El Secretario General del honorable Senado de la República,

Manuel Enríquez Rosero.

El Presidente de la honorable Cámara de Representantes,

Emilio Martínez Rosales.

El Secretario General de la honorable Cámara de Representantes,

Gustavo Bustamante Moratto.

REPUBLICA DE COLOMBIA – GOBIERNO NACIONAL

Publíquese y ejecútese.

Dada en Santa Fe de Bogotá, D. C., a 18 de agosto de 1999.

ANDRES PASTRANA ARANGO

El Ministro de Desarrollo Económico,

Fernando Araújo Perdomo.

La Ministra de Comercio Exterior,

Martha Lucía Ramírez de Rincón.

La Ministra de Comunicaciones,

Claudia De Francisco Zambrano.

El Ministro de Transporte,

Mauricio Cárdenas Santamaría.