SPI-ISS-02-11

DIRECCIÓN DE SERVICIOS DE INVESTIGACIÓN Y ANÁLISIS

Subdirección de Política Interior

LXI LEGISLATURA
CÁMARA DE DIPUTADOS

Centro de Documentación, Información y Análisis

FIRMA ELECTRÓNICA AVANZADA

Análisis de la Iniciativa Presentada por el Ejecutivo Federal, Derecho Comparado y Opiniones Especializadas en el Tema.

Mtra. Claudia Gamboa Montejano
Investigadora Parlamentaria

Enero, 2011.

Av. Congreso de la Unión Núm. 66; Col. El Parque; Delegación Venustiano Carranza;
C.P. 15969 México, DF; Teléfono: 50360000 extensiones: 67033, 67036 y 67026
E-mail: claudia.gamboa@congreso.gob.mx

“FIRMA ELECTRÓNICA AVANZADA
Análisis de la Iniciativa Presentada por el Ejecutivo Federal, Derecho Comparado y Opiniones Especializadas en el Tema”.

INDICE

INTRODUCCIÓN

Los distintos avances tecnológicos que se han generado en los últimos años, han sido cada vez más revolucionarios, desde el punto de vista de sus alcances en la modificación de las actividades humanas, ocasionando con ello que a nivel mundial, las personas dentro del contexto denominado *"sociedad de la información"*, dependa cada vez más de los sistemas informáticos, así como de los productos y servicios que éstos generan, para una mayor comodidad y facilidad en sus distintas tareas cotidianas.

Muchas de estas actividades humanas, trasladadas al ámbito del Derecho, tienen trascendencia que derivan en actos jurídicos propios, los cuales conjugados con la tecnología, propician una nueva plataforma de acción técnico-jurídica, es así que se ha creado en los umbrales del siglo XXI,- ya en muchos países, incluyendo el nuestro-, lo que se conoce como la firma electrónica avanzada (FEA), a través de la cual se pretende generalizar los lineamientos entre distintas formas de obtener ciertos servicios, ya sea entre los particulares, así como entre éstos y la administración pública.

Es así, que a través de la iniciativa presentada por el Ejecutivo Federal el 9 de diciembre ante la Cámara de Senadores, se pretende extender y unificar los distintos lineamientos relacionados a la Firma Electrónica Avanzada, entre ellos la especificación de las autoridades certificadoras, los procedimientos que habrán de llevarse a cabo, así como los requisitos para ello, ya que si bien son ya varias las leyes que contemplan la utilización de dicho sistema de identificación, aún no están establecidos a nivel general los distintos aspectos técnico-legales para su implementación.

Cabe señalar que la propia iniciativa denomina a la Firma Electrónica Avanzada como *"el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, y que produce los mismos efectos jurídicos que la firma autógrafa"*.

Un elemento muy importante en este proceso técnico es la llamada certificación que hace una autoridad determinada de que en verdad se esté tratando de la persona quien dice ser, lo que conlleva un sistema de confiabilidad mucho más seguro. La presentación de esta iniciativa de ley en la materia por parte del Ejecutivo, viene a reforzar la idea de globalidad y necesidad de interconexión de los distintos sujetos que hoy en día interactúan a nivel mundial, ya sea por negocios o por distintas circunstancias, facilitando con esto las distintas actividades humanas, pero con cierto grado de tecnicismo.

RESUMEN EJECUTIVO

En el desarrollo de este trabajo de análisis relativo a la propuesta del Ejecutivo Federal, en materia de la firma electrónica avanzada, se exponen los siguientes apartados:

En el **MARCO CONCEPTUAL** se definen entre otros, los siguientes términos: firma, firma electrónica, clasificación de la firma electrónica, conceptos relacionados con la firma electrónica, características de un sistema seguro.

EXTRACTO DEL TEXTO DE LA EXPOSICIÓN DE MOTIVOS. En este rubro de muestra la principal argumentación empleada por el Ejecutivo Federal para proponer la creación de esta legislación en concreto.

ANÁLISIS DEL TEXTO PROPUESTO. Se muestra el contenido por la iniciativa, separado por Títulos, señalando al final de cada uno de éstos, los datos relevantes correspondientes.

DERECHO COMPARADO. En este rubro, se muestra la estructura (índice) de la legislación existente en materia de firma electrónica avanzada de los países de: Argentina, Chile, España, Perú y Venezuela, señalando posteriormente las aportaciones en específico de cada país al respecto.

OPINIONES ESPECIALIZADAS. Se muestran las distintas opiniones y comentarios que hacen diversos especialistas en la materia, enfatizando los realizados en España, país pionero en la regulación de la firma electrónica.

Al final del documento se agrega un **ANEXO**, denominado “Aplicaciones de la Firma Electrónica”, considerándolo oportuno por el tecnicismo del tema informático abordado en este caso.

MARCO CONCEPTUAL.

En primera instancia se hace referencia a conceptos relacionados con el tema de la firma electrónica, los cuales permitirán contar con una mayor visión y certidumbre de lo que versa la iniciativa materia de análisis.

Comenzaremos por señalar en qué consiste la firma, desde un punto de vista legal:

[1]**DEFINICION LEGAL DE LA FIRMA**.

"Siguiendo el mismo hilo conductor, y a la vista de que conocemos ya las funciones, debemos contrastar las mismas con el significado que tiene la firma como tal, ya que no debemos olvidar que, a fin de cuentas, ésta no es más que una nueva modalidad de avalar documentos, tanto en el significado lego como en el jurídico, ya que este sistema tiene como objetivo traspolar los efectos jurídicos de una firma tradicional al campo de la electrónica, …

Como primer punto, debemos pues, remitirnos a las definiciones aceptadas por los diccionarios de la lengua española respecto de la firma, de las cuales he descartado intencionalmente aquellas no referidas a la firma como elemento integrante de un documento debido a la exposición previa sobre las funciones de la firma, que me permite dicha licencia.

Firma. Nombre y apellido que una persona pone, con rúbrica o sin ella, al pie de un escrito como señal de autenticidad.

Firma. Autorizar un escrito o documento con la firma.

Las definiciones presentadas aceptan la idea de lo que es la firma en su significado *lato sensu*, pero los tratadistas Planiol y Riper la definen de la siguiente manera: "la firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto"

…".

Ahora bien, entrando en materia, y señalando específicamente lo que se entiende por firma electrónica, así como todo lo que ello implica, se señala así lo siguiente:

[1] La Firma Electrónica en el Régimen Comercial Mexicano Gabriel Andrés Cámpoli Editorial Porrúa. México, 2004. Pags. 2 y 3.

[2]Firma Electrónica.

"El documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica. La seguridad en el comercio electrónico es fundamental para su desarrollo. En un flujo de transacciones en donde las partes ya no tienen contacto 'físico', ¿cómo pueden asegurarse de la identidad de aquel con quien están realizando una operación? e, incluso, ¿cómo pueden tener la certeza de que la información intercambiada no ha sido robada, alterada o conocida por personas ajenas?

La firma electrónica, técnicamente, es un conjunto o bloque de caracteres que viaja junto a un documento, fichero o mensaje y que puede acreditar cuál es el autor o emisor del mismo (lo que se denomina autenticación) y que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación (o integridad).

Es aquél conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, contenido en un soporte magnético ya sea en un disquete, algún dispositivo externo o disco duro de una computadora y no de papel), que permite identificar a su autor, es decir que es el conjunto de datos, en forma electrónica, anexos 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.

La Firma Electrónica permite identificar a la persona que realiza la transacción, es decir, proporciona el servicio de autentificación (verificación de la autoridad del firmante para estar seguro de que fue él y no otro el autor del documento) y no de repudio (seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones asignadas en él).

Quizás la parte que más nos interesa a los usuarios es la garantía de detección de cualquier modificación de los datos firmados, proporcionando una integridad total ante alteraciones fortuitas o deliberadas durante la transmisión telemática del documento firmado. El hecho de la firma sea creada por el usuario mediante medios que mantiene bajo su propio control (clave privada protegida, contraseña, datos biométricos, tarjeta chip, etc.) asegura la imposibilidad de efectuar de lo que se conoce como "suplantación de personalidad".

En otras palabras podríamos definir a la Firma Electrónica como el conjunto de datos, en forma electrónica, anexos 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. La debilidad en cuanto al emisor y al receptor radica en la posible suplantación de la identidad de alguno de ellos por parte de elementos ajenos al sistema.

[2] Reyes Krafft, Alfredo Alejandro. "La Firma Electrónica y las entidades de certificación". Editorial Porrúa. México, 2003. Pags. 175 a la 178.

> Para evitar estos problemas, existen dos tipos de soluciones tecnológicas: el cifrado de los datos y la firma electrónica. Con el primero se puede transformar un texto claro en otro completamente ininteligible, que aun capturado sea prácticamente imposible de adivinar. Con la segunda, se consigue garantizar que quien envía los datos es realmente quien dice ser y no otro, y que dichos datos no han sido manipulados por el camino.
> …
> Criptografía es la ciencia de mantener en secreto los mensajes. El texto original, o texto puro es convertido en un equivalente en códigos, llamado criptotexto (ciphertext) via un algoritmo de encripción. El criptotexto es decodificado (decriptado) al momento de su recepción y vuelve a su forma de texto original.
> La criptología se define como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Abarca por tanto a la Criptografía (datos, textos e imágenes), Criptofonía (voz) y al Criptoanálisis (ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave)".

El mismo autor, menciona la gran clasificación que actualmente se hace de la firma electrónica, siendo ésta la siguiente:

CLASIFICACIÓN DE LA FIRMA ELECTRÓNICA.

[3]La firma electrónica se puede clasificar de la siguiente manera:

Simple definida como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes) o

Avanzada que podemos conceptuar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste (entendida como proceso electrónico que permite al receptor de un mensaje de datos identificar formalmente a su autor, el cual mantiene bajo su exclusivo control los medios para crear dicha firma), de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

[3] Ibidem. Pags. 246 y 247.

Debemos distinguir entre lo que comúnmente se denomina “firma digital” y la “firma electrónica avanzada”, ya que la primera es una especie de la segunda, esto es, la firma digital es una firma electrónica avanzada elaborada bajo los estándares de la tecnología digital.

Con el propósito de abordar otros elementos que intervienen en el procedimiento de creación y utilización de la firma electrónica como tal, se hace referencia a los siguientes aspectos:

[4]CONCEPTOS RELACIONADOS CON LA FIRMA ELECTRÓNICA

MENSAJE DE DATOS
Debemos entender primeramente el concepto de mensaje de datos que es la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares como son el intercambio electrónico de datos, el correo electrónico, telegrama, telex o telefax. El mensaje de datos no se limita a sólo comunicación sino que pretende abarcar cualquier tipo de información respaldada en un soporte de tipo informático que no necesariamente este destinada a ser comunicada, así el concepto de mensaje incluye el de información meramente consignada.

INTERCAMBIO ELECTRÓNICO DE DATOS (EDI)
Es la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convencida al efecto.

INICIADOR DE UN MENSAJE DE DATOS
Aquella persona que, al tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él.

DESTINATARIO DE UN MENSAJE DE DATOS
Aquella persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él.

INTERMEDIARIO DE UN MENSAJE DE DATOS
La persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

EQUIVALENCIA FUNCIONAL
La Ley Modelo de las Naciones Unidas se basa en el reconocimiento de que los requisitos legales que prescriben el empleo de la documentación tradicional con soporte de papel constituyen el principal obstáculo para el desarrollo de los medios modernos de comunicación. De modo que la Ley Modelo sigue el principio conocido como “criterio de equivalente funcional”, basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones a través de medios electrónicos.

[4] Ibidem. Pags. 164 a 170.

Es decir, ese documento de papel cumple funciones como las siguientes:

- Proporcionar un texto legible para todos.
- Asegurar la inalterabilidad de un mensaje a lo largo del tiempo.
- Permitir su reproducción a fin de que cada una de las partes disponga de un ejemplar del mismo.
- Permitir la autenticación de los datos consignados suscribiéndolos con una firma y
- Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales.

Cabe señalar que respecto de todas esas funciones, la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor confiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, siempre y cuando se observen ciertos requisitos técnicos y jurídicos.

AUTORIDAD O ENTIDAD DE CERTIFICACIÓN

La creciente interconexión de los sistemas de información, posibilitada por la general aceptación de los sistemas abiertos, y las cada vez mayores prestaciones de las actuales redes de telecomunicación, obtenidas principalmente de la digitalización, están potenciando formas de intercambio de información impensables hace pocos años. A su vez, ello está conduciendo a una avalancha de nuevos servicios y aplicaciones telemáticas, con un enorme poder de penetración en las emergentes sociedades de la información. Así, el teletrabajo, la teleadministración, el comercio electrónico, etc., están modificando revolucionariamente las relaciones económicas, administrativas, laborales de tal forma que en pocos años serán radicalmente distintas de cómo son ahora.

Todos estos nuevos servicios y aplicaciones no podrán desarrollarse en plenitud a no ser que se les dote de unos servicios y mecanismos de seguridad fiables.

Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento a seguir.

AUTENTICACIÓN

Prueba o garantía de la identidad de quien envía la información, es decir que es el proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros, lo cual desarrollo en párrafos subsecuentes.

Hace referencia a la utilización de la firma digital con el fin de verificar la identidad del remitente del mensaje de datos. Aquí se puede plantear el supuesto de que un determinado sujeto A publique una clave pública con un nombre falso; el destinatario de un mensaje enviado por A, pensará que la identidad del emisor es A, sin embargo esto no es cierto, puesto que su verdadera identidad es P: el emisor del mensaje de datos no es quien dice ser, sino que se trata de otra persona. Ante la posibilidad de que se den casos como el expuesto, es probable que el receptor de un mensaje desee una información más fidedigna sobre la identidad del titular de la clave, del emisor del mensaje; esta información la puede facilitar el emisor mediante cualquier tipo de prueba que el receptor considere contundente, o se puede verificar la identidad del emisor mediante la confirmación de la misma por una tercera persona (autoridades de certificación, por lo general).

CARACTERÍSTICAS DE UN SISTEMA SEGURO

SERVICIOS DE SEGURIDAD	DEFINICIÓN	MECANISMOS DISPONIBLES
Autenticación	Prueba o garantía de la identidad de quien envía la información	User-Password Tarjeta Inteligente Huella Digital
Control de Acceso	Permisos diferenciados de acceso a Segmentos y necesidades específicas por cliente	Perfiles de Usuario
Confidencialidad	Garantía de que el contenido de la información se mantiene oculta salvo para el destinatario	Algoritmos de encripción con llaves públicas y privadas
Integridad	Garantía de que el contenido del mensaje no sufrió ninguna modificación	Algoritmos de encripción con llaves públicas y privadas
No repudiación	Inhabilidad de un individuo para desconocer una transacción una vez realizada	Algoritmos de encripción con llaves públicas y privadas

De acuerdo a la anterior información, respecto a lo que conlleva la instauración homogénea de la firma electrónica en nuestro país, se puede advertir una serie de cuestiones muy técnicas, las cuales es necesario comprender y asimilar con el propósito de entender mejor la dinámica que se propone para este tipo de asuntos informáticos, que si bien por una parte permiten mayor prontitud y exactitud en la información que se intercambia, -principalmente entre determinados entes públicos y la ciudadanía-, por otra parte resulta muy novedosos, pero complejo, por lo que habrá que irse adecuando a la nueva forma de protocolización de ciertos actos jurídicos, a través de esta nueva forma de aceptación de derechos y obligaciones.

EXTRACTO DEL TEXTO DE LA EXPOSICIÓN DE MOTIVOS.

Se presenta a continuación los principales extractos contenidos en la argumentación de la iniciativa de ley de la Firma Electrónica Avanzada.

[5]"…

En el ámbito del derecho comparado, las experiencias normativas de los Estados Unidos de América, España y Chile, aportan elementos jurídicos que han favorecido su integración en la Sociedad de la información y que, de ser adaptados al contexto y tradición jurídica nacional e incorporados en la normatividad mexicana, pueden aportar importantes beneficios para los ciudadanos, las empresas e instituciones públicas.

De ahí, que al considerar la tendencia creciente en el ámbito mundial hacia el uso de medios de comunicación electrónica en la prestación de todo tipo de trámites y servicios, así como la experiencia positiva obtenida en los últimos años en nuestro país en esta materia, se refuerza la convicción del Ejecutivo Federal a mi cargo de que el uso de las tecnologías de la información y comunicaciones en la gestión pública es una opción que debe impulsarse para generar condiciones que permitan hacer más efectiva la provisión de trámites, servicios y procedimientos públicos.

Para ello, la iniciativa que se presenta, busca mediante el aprovechamiento de los medios de comunicación electrónica, optimizar y ampliar el acceso y la cobertura a los diferentes trámites y servicios gubernamentales que se proporcionan a la sociedad, así como para lograr una verdadera administración pública "en línea" que permita comunicar a los servidores públicos entre sí y facilitar la interacción entre el gobierno y los ciudadanos, evitando así que éstos realicen desplazamientos innecesarios a los lugares en que se ubican las instituciones públicas, con el consecuente abatimiento de los costos en que incurren los particulares por los traslados y el Gobierno Federal en el uso de papelería.

Lo anterior, independientemente de que la mejora de los trámites y servicios públicos, así como de los procedimientos administrativos necesariamente inhibirá la posibilidad de que se presente la práctica de actos de corrupción, reducirá la discrecionalidad y arbitrariedad e incrementará la transparencia en la gestión gubernamental.

Es de resaltar, que el uso de medios de comunicación electrónica no es ajeno al sistema jurídico mexicano, ya que actualmente diversos ordenamientos legales de carácter federal reconocen el uso de la firma electrónica avanzada y de su certificado digital o bien, el empleo de medios de identificación electrónica en actos jurídicos realizados a través de medios electrónicos, entre otros, el Código de Comercio, el Código Fiscal de la Federación, el Código Civil Federal, la Ley Federal de Procedimiento Administrativo, la Ley Federal de Procedimiento Contencioso Administrativo, la Ley Aduanera , la Ley de Comercio Exterior, la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la Ley de Obras Públicas y Servicios Relacionados con las Mismas, la Ley Federal de Protección al Consumidor, la Ley del Seguro Social, la Ley Federal para el Control de Sustancias

[5]Iniciativa del Ejecutivo que propone la creación de la Ley de Firma Electrónica Avanzada, presentada ante el Senado de la República el 9 de diciembre del 2010. Dirección en Internet: http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=6754&lg=61

Químicas Susceptibles de Desvío para la Fabricación de Armas Químicas, la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa y la Ley de Instituciones de Crédito.

En el orden estatal, las legislaturas de los estados de Colima, Guanajuato, Hidalgo, Jalisco, Sonora y Yucatán, así como la Asamblea Legislativa del Gobierno del Distrito Federal han impulsado la emisión de leyes especiales para reconocer el uso de la firma electrónica en los trámites, servicios, actos y procedimientos administrativos que los particulares efectúen ante las diferentes dependencias y entidades de la Administración Pública Local, los órganos estatales autónomos e incluso ante sus respectivos poderes Legislativo y Judicial, a través de medios de comunicación electrónica.

Es importante destacar que algunas dependencias y entidades de la Administración Pública Federal han realizado esfuerzos importantes para promover el uso de estos medios en las diversas actividades que realizan, entre ellos, la publicación en el Diario Oficial de la Federación, el 9 de diciembre de 2005, del Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, cuya finalidad es promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones entre las dependencias y entidades de la Administración Pública Federal. En el Acuerdo señalado, destaca también la creación de la Subcomisión de Firma Electrónica Avanzada, integrada por los representantes designados por los Titulares de las secretarías de Economía (SE) y de la Función Pública (SFP), así como del Servicio de Administración Tributaria (SAT).

Entre las funciones más relevantes con que cuenta la referida Subcomisión, se encuentra la de coordinar las acciones necesarias para la homologación de la firma electrónica avanzada en la Administración Pública Federal; para ello, con fecha 24 de agosto de 2006, se publicó en el referido órgano de difusión oficial el Acuerdo Interinstitucional por el que se establecen los Lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, mediante los cuales se ha buscado evitar la duplicidad o multiplicidad de certificados digitales de firma electrónica avanzada asociados a una misma persona, así como establecer el reconocimiento de los mismos por las autoridades certificadoras de las dependencias, entidades y prestadores de servicios de certificación.

En este sentido, y por lo que se refiere al ámbito mercantil, la SE con motivo de las reformas al Código de Comercio, publicadas en el Diario Oficial de la Federación el 29 de mayo de 2000, está encargada de administrar el sistema de información y custodiar la base de datos central del Registro Público de Comercio (RPC), y desde el año 2005, de la infraestructura de Clave Pública de Prestadores de Servicios de Certificación.

Bajo ese contexto, corresponde a la citada Secretaría, por mandato legal, certificar las claves públicas de los responsables del RPC y de los fedatarios públicos, específicamente corredores y notarios públicos, así como certificar, a través de los PSC, las claves públicas de personas físicas o morales que son acreditadas por la propia Secretaría, en virtud de que su política de certificados resulta consecuente con los ordenamientos aplicables y su uso está orientado para actos de comercio.

Es importante resaltar, que los sistemas y bases de datos antes mencionados han sido diseñados bajo un esquema de seguridad que considera políticas y procedimientos, así como dispositivos y software de seguridad que involucran exitosamente la firma

electrónica y los certificados digitales. Con esto, el Gobierno Federal ha hecho posible, por primera vez en México, la prestación cotidiana e ininterrumpida de un servicio público utilizando medios de comunicación electrónica, aprovechando las ventajas que ofrecen los esquemas tecnológicos actuales que, además, dotan de seguridad a esas transacciones y, por tanto, se encuentran plenamente reconocidos en el orden jurídico mexicano.

…

En otro orden de ideas, es de hacer notar que para efectos de la Iniciativa que se presenta, se excluyen expresamente de la aplicación de esta Ley, los actos relacionados con las materias fiscal y aduanera, en virtud de que tienen como objetivo proveer al Estado de los recursos necesarios para su funcionamiento, así mismo se excluye la materia financiera cuyo objetivo es regular a las instituciones financieras en el desarrollo de sus actividades. Lo anterior, a efecto de responder de manera ágil y oportuna a las cambiantes condiciones de la economía, de forma que se asegure siempre la adecuada obtención de los recursos públicos y mantener la estabilidad del sistema financiero, considerando el incremento cada vez mayor del número y montos de las transferencias electrónicas de dinero y valores.

No obstante lo anterior, la iniciativa reconoce la importancia de la participación del SAT, como autoridad certificadora, para la expedición de certificados digitales en términos de la Ley que se propone emitir.

Por su parte, la SFP en ejercicio de las atribuciones que tiene conferidas en materia de registro de situación patrimonial de los servidores públicos de la Administración Pública Federal, ha implementado el uso obligatorio de la firma electrónica avanzada, para facilitar el cumplimiento por parte de los servidores públicos que, en términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, deben presentar diversas declaraciones.

Asimismo, de acuerdo con las leyes de Adquisiciones, Arrendamientos y Servicios del Sector Público, y de Obras Públicas y Servicios Relacionados con las Mismas, la SFP es la dependencia encargada de operar el sistema de certificación de los medios de identificación electrónica que utilicen las dependencias, entidades o los licitantes.

Acorde con lo antes expuesto, la SFP ha desarrollado diversos servicios electrónicos transversales, tales como: Compranet, Tramitanet y el Registro Único de Personas Acreditadas, en los que se ha implantado el uso de la firma electrónica, con lo cual se han obtenido ahorros importantes en tiempo, recursos humanos y económicos.

Adicionalmente, la SFP está trabajando conjuntamente con diversas dependencias y entidades de la Administración Pública Federal en la implantación de la firma electrónica avanzada en más de cien trámites de alto impacto para la ciudadanía.

Cabe destacar que, desde el año 2000 y hasta la fecha, la SFP ha emitido más de un millón de certificados de firma electrónica, como parte de su estrategia para mejorar la regulación, la gestión, los procesos y los resultados de la Administración Pública Federal para satisfacer las necesidades de los ciudadanos, así como para incrementar los estándares de eficiencia y eficacia gubernamental, a través del aprovechamiento de las tecnologías de la información y comunicaciones y así, elevar el desarrollo del Gobierno Digital.

Es pertinente hacer notar que no obstante las acciones y esfuerzos que se han realizado en el ámbito de la Administración Pública Federal, a la fecha no se ha logrado el uso generalizado de la firma electrónica avanzada como una herramienta indispensable en el desarrollo de las actividades entre las instituciones públicas y entre

éstas con los particulares, por lo que se requiere de la expedición de un ordenamiento legal en el que se regule de manera uniforme la firma electrónica avanzada que utilicen los servidores públicos y los particulares en los actos regulados por el derecho público que se lleven a cabo a través de medios electrónicos, a fin de proporcionarles plena certeza sobre la seguridad jurídica y fiabilidad técnica con respecto a dichos actos, propiciar así la integración de nuestro país en la Sociedad de la Información.

Además, el uso de la Firma electrónica coadyuvará a la mejor y más pronta implementación de políticas públicas dirigidas a la conversación y preservación del medio ambiente, particularmente el ahorro y utilización de papel, que ya se encuentra previsto en el Decreto por el que se establecen diversas medidas en materia de adquisiciones, uso de papel y de la certificación de manejo sustentable de bosques por la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 05 de septiembre de 2007.

La generación de trámites a través de mecanismos electrónicos, empleando los avances tecnológicos y las plataformas informáticas constituyen una más de las estrategias que nos permiten el uso de cada vez menos papel e importante ahorros tanto para el sector público como el privado.

…".

ANÁLISIS DEL TEXTO PROPUESTO.

La iniciativa de Ley que se presenta a su consideración se estructura en treinta y un artículos desarrollados en cuatro títulos.

INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE EXPIDE LA LEY DE FIRMA ELECTRÓNICA AVANZADA

TEXTO PROPUESTO

TÍTULO PRIMERO
DISPOSICIONES GENERALES
CAPÍTULO ÚNICO

ARTÍCULO 1.- La presente Ley es de orden e interés público y tiene por objeto regular:

I. El uso de la firma electrónica avanzada en los actos previstos en esta Ley y la expedición de certificados digitales a personas físicas;

II. Los servicios relacionados con la firma electrónica avanzada, en los términos establecidos en esta Ley, con las firmas electrónicas avanzadas reguladas por otros ordenamientos legales.

ARTÍCULO 2.- Para los efectos de la presente Ley se entenderá por:

I. **Actos:** las comunicaciones, trámites, servicios, actos jurídicos y administrativos, así como los procedimientos administrativos en los cuales los particulares y los servidores públicos de las dependencias y entidades de la Administración Pública Federal, de la Procuraduría General de la República y de las unidades administrativas de la Presidencia de la República, utilicen la firma electrónica avanzada;

II. **Actuaciones Electrónicas:** las notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes o documentos y, en su caso, las resoluciones administrativas definitivas que se emitan en los actos que se refiere esta Ley y que se comuniquen por medios electrónicos;

III. **Acuse de Recibo Electrónico:** el mensaje de datos que se emite o genera a través de medios de comunicación electrónica para acreditar de manera fehaciente la fecha y hora de recepción de documentos electrónicos relacionados con los actos establecidos por esta Ley;

IV. **Autoridad Certificadora:** las dependencias y entidades de la Administración Pública Federal y los prestadores de servicios de certificación que, conforme a las disposiciones jurídicas, tengan reconocida esta calidad y cuenten con la infraestructura tecnológica para la emisión, administración y registro de certificados digitales, así como para proporcionar servicios relacionados con los mismos;

V. **Certificado Digital:** el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada;

VI. **Clave Privada:** los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante.

VII. **Clave Pública:** los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante;

VIII. **Datos y elementos de identificación:** aquellos que se encuentran considerados como tales en la Ley General de Población y en las disposiciones que deriven de la misma;

IX. **Dependencias:** las secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como las unidades administrativas de la Presidencia de la República, conforme a lo dispuesto en la Ley

Orgánica de la Administración Pública Federal. La Procuraduría General de la República será considerada con este carácter para efectos de los actos administrativos que realice en términos de esta Ley;

X. **Documento Electrónico:** aquél que es generado, consultado, modificado o procesado por medios electrónicos;

XI. **Dirección de Correo Electrónico:** la dirección en Internet señalada por los servidores públicos y particulares para enviar y recibir mensajes de datos y documentos electrónicos relacionados con los actos a que se refiere la presente Ley, a través de los medios de comunicación electrónica;

XII. **Entidades:** los organismos públicos descentralizados, empresas de participación estatal mayoritaria y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;

XIII. **Firma Electrónica Avanzada:** el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, y que produce los mismos efectos jurídicos que la firma autógrafa;

XIV. **Firmante:** toda persona que utiliza su firma electrónica avanzada para suscribir documentos electrónicos y, en su caso, mensajes de datos;

XV. **Medios de Comunicación Electrónica:** los dispositivos tecnológicos que permiten efectuar la transmisión y recepción de mensajes de datos y documentos electrónicos;

XVI. **Medios Electrónicos:** los dispositivos tecnológicos para el procesamiento, impresión, despliegue, conservación y, en su caso, modificación de información;

XVII. **Mensaje de Datos:** la información generada, enviada, recibida, archivada o comunicada a través de medios de comunicación electrónica, que puede contener documentos electrónicos;

XVIII. **Página Web:** el sitio en Internet que contiene información, aplicaciones y, en su caso, vínculos a otras páginas;

XIX. **Prestador de Servicios de Certificación:** las instituciones públicas conforme a las leyes que son aplicables, así como los notarios y corredores públicos y las personas morales de carácter privado que de acuerdo a lo establecido en el Código de Comercio sean reconocidas con tal carácter para prestar servicios relacionados con la firma electrónica avanzada, y en su caso, expedir certificados digitales;

XX. **Secretaría:** la secretaría de la Función Pública;

XXI. **Servicios Relacionados con la Firma Electrónica Avanzada:** los servicios de firmado de documentos electrónicos, de verificación de la vigencia de certificados digitales, de verificación y validación de la unicidad de la clave pública, así como de consulta de certificados digitales revocados, entre otros, que en términos de las disposiciones jurídicas aplicables pueden ser proporcionados por la autoridad certificadora;

XXII. **Sistema de Trámites Electrónicos:** el sitio desarrollado por la dependencia o entidad para el envío y recepción de documentos, notificaciones y comunicaciones, así como para la consulta de información relacionada con los actos a que se refiere esta Ley, contenido en la página Web de la propia dependencia o entidad;

XXIII. **Sujetos Obligados:** los servidores públicos y particulares que utilicen la firma electrónica avanzada, en términos de lo previsto en las fracciones II y III del artículo 3 de esta Ley, y

XXIV. **Tablero Electrónico:** el medio electrónico a través del cual se ponen a disposición los particulares que utilicen la firma electrónica avanzada en términos de esta ley, las

actuaciones electrónicas que emitan las dependencias y entidades, y que genera un acuse de recibo electrónico.

Este medio electrónico estará ubicado en el sistema de trámites electrónicos de las propias dependencias y entidades.

ARTÍCULO 3.- Están sujetos a las disposiciones de la presente Ley:

I. Las dependencias y entidades;
II. Los servidores públicos de las dependencias y entidades que en la realización de los actos a que se refiere esta Ley utilicen la firma electrónica avanzada, y
III. Los particulares, en los casos en que utilicen la firma electrónica avanzada en términos de esta Ley.

ARTÍCULO 4.- Las disposiciones de esta Ley no serán aplicables a los actos en que no sea factible el uso de la firma electrónica avanzada por disposición de ley o aquellos en que exista previo dictamen de la Secretaría. Tampoco serán aplicables a las materias fiscal, aduanera y financiera.

En los actos de comercio e inscripciones en el Registro Público de Comercio, el uso de la firma electrónica avanzada se regirá de conformidad con lo previsto en el Código de Comercio y demás ordenamientos aplicables en la materia, sin perjuicio de la aplicación de los dispuesto en esta Ley en lo que resulte procedente.

ARTÍCULO 5.- La Secretaría, en el ámbito de su competencia, estará facultada para interpretar las disposiciones de esta Ley para efectos administrativos.

La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria dictarán, de manera conjunta, las disposiciones generales para el adecuado cumplimiento de esta Ley, mismas que deberán publicarse en el Diario Oficial de la Federación.

ARTÍCULO 6.- A falta de disposición expresa en esta Ley o en las demás disposiciones que de ella deriven, se aplicarán supletoriamente la Ley Federal de Procedimiento Administrativo, el Código Civil Federal y el Código Federal de Procedimientos Civiles.

Datos Relevantes:

El titulo primero de esta Ley aborda su objetivo, el cual radica en regular el uso de la firma electrónica y los servicios que tengan que ver con la misma. Posteriormente para otorgar una mayor claridad sobre lo que esta Ley pretende regular, se resalta una serie de conceptos afines a la Ley que sin duda es indispensable conocer para evitar confusiones o malinterpretaciones posteriores, más tratándose de un tema tan técnico a nivel informático, entre estos conceptos tenemos lo que se refiere a actuaciones electrónicas, clave privada, clave pública, dependencias, autoridades certificadoras, firma electrónica avanzada por solo mencionar algunos ejemplos.

También en este título se señalan los sujetos que tendrán que acatar esta ley, los cuales son las dependencias y entidades, los servidores públicos de estas así como los particulares. Cabe mencionar que se resalta que estas disposiciones **no serán aplicables a las materias fiscal, aduanera y financiera.** Se indica que de manera conjunta tanto la Secretaría de Economía y el Servicio de Administración Tributaria dictarán las disposiciones generales para que esta Ley sea llevada a cabo de manera uniforme.

Finalmente este título primero también aborda bajo qué criterios se regirá esta Ley, es decir en caso de un acto de omisión o falta a esta. Estos son: la Ley Federal de Procedimiento Administrativo, el Código Civil Federal y el Código Federal de Procedimientos Civiles.

TITULO SEGUNDO
DE LA FIRMA ELECTRÓNICA AVANZADA
CAPÍTULO I
Del uso y validez de la firma electrónica avanzada

ARTÍCULO 7.- La firma electrónica avanzada podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos.

Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.

ARTÍCULO 8.- Para afectos del artículo 7 de esta Ley, la firma electrónica avanzada debería cumplir con los principios rectores siguientes:

I. **Equivalencia Funcional:** la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos;
II. **Autenticidad:** la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;
III. **Integridad:** la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;
IV. **Neutralidad Tecnológica:** la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;
V. **No Repudio:** la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y
VI. **Confidencialidad:** la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

ARTÍCULO 9.- Para que los sujetos obligados puedan utilizar la firma electrónica avanzada en los actos a que se refiere esta Ley deberán contar con:

I. Un certificado digital vigente, emitido y homologado en términos de la presente Ley, y
II. Una clave privada, generada bajo su exclusivo control.

CAPITULO II
De los documentos electrónicos y de los mensajes de datos

ARTÍCULO 10.- Las dependencias y entidades en las comunicaciones y, en su caso, actos jurídicos que realicen entre las mismas, harán uso de mensajes de datos y aceptarán la presentación de documentos electrónicos, los cuales deberán contar, cuando así se requiera, con la firma electrónica avanzada del servidor público facultado para ello.

ARTÍCULO 11.- Las dependencias y entidades en la realización de los actos a que se refiere

esta Ley deberán aceptar el uso de mensajes de datos y la presentación de documentos electrónicos cuando las mismas ofrezcan esta posibilidad, siempre que los particulares por si o, en su caso, a través de las personas autorizadas por los mismos en términos del artículo 19 de la Ley Federal de Procedimiento Administrativo, manifiesten expresamente su conformidad para que dichos actos se efectúen, desde su inicio hasta su conclusión, a través de medios de comunicación electrónica.

La manifestación a que se refiere el párrafo anterior deberá señalar adicionalmente:

I. Que aceptan consultar el tablero electrónico, al menos, los días quince y último de cada mes o bien, el día hábil siguiente si alguno de éstos fuere inhábil; y en caso de no hacerlo, se tendrá por hecha la notificación en el día hábil que corresponda;

II. Que aceptan darse por notificados de las adecuaciones electrónicas que emita la dependencia o entidad que corresponda, en el mismo día que consulten el tablero electrónico, y

III. Que el supuesto de que por causas imputables a la dependencia o entidad se encuentren imposibilitados para consultar el tablero electrónico o abrir los documentos electrónico que contengan la información depositada en el mismo, en los días señalados en la fracción I de este artículo, lo harán del conocimiento de la propia dependencia o entidad a más tardar dentro de los tres días hábiles siguientes a aquél en que ocurra dicho impedimento, por medios de comunicación electrónica o cualquier otro previsto en el Reglamento de esta Ley, para que sean notificados por alguna otra forma de las establecidas en la Ley Federal de Procedimiento Administrativo.

ARTÍCULO 12.- Los sujetos obligados deberán contar con una dirección de correo electrónico para recibir, cuando corresponda, mensajes de datos y documentos electrónicos en la realización de los actos previstos en esta Ley.

ARTÍCULO 13.- Cada dependencia y entidad creará y administrará un sistema de trámites electrónicos que establezca en control de accesos, los respaldos y la recuperación de información, con mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia.

La Secretaría emitirá los lineamientos conducentes a efecto de dar cumplimiento a lo dispuesto en este artículo.

ARTÍCULO 14.- La información contenida en los mensajes de datos y en los documentos electrónicos será pública, salvo que la misma esté clasificada como reservada o confidencial en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Los mensajes de datos y los documentos electrónicos que contengan datos personales estarán sujetos a las disposiciones aplicables al manejo, seguridad y protección de los mismos.

ARTÍCULO 15.- Las dependencias y entidades, así como los sujetos obligados deberán conservar en medios electrónicos, los mensajes de datos y los documentos electrónicos con firma electrónica avanzada derivados de los actos a que se refiere esta Ley, durante los plazos de conservación previstos en los ordenamientos aplicables, según la naturaleza de la información.

Mediante disposiciones generales se establecerá lo relativo a la conservación de los mensajes de datos y de los documentos electrónicos con firma electrónica avanzada, para lo cual se tomarán en cuenta, entre otros requisitos, los previstos en la Norma Oficial Mexicana a que se refiere el artículo 49 del Código de Comercio.

ARTÍCULO 16.- Cuando se requiera que un documento impreso y con firma autógrafa, sea presentado o conservado en su forma original, tal requisito quedará satisfecho si la copia se genera en un documento electrónico, y se cumple con lo siguiente:

I. Que la migración a una forma digital haya sido realizada o supervisada por un servidor público que cuente con facultades de certificación de documentos en términos de las disposiciones aplicables o, en su caso, por el particular interesado, quién deberá manifestar, bajo protesta de decir verdad, que el documento electrónico es copia íntegra e inalterada del documento impreso;
II. Cuando exista duda sobre la autenticidad de documento electrónico remitido, la dependencia o entidad podrá solicitar que el documento impreso le sea presentado directamente o bien, que éste último se le envíe por correo certificado con acuse de recibo.
En el supuesto de que se opte por el envío del documento impreso a través del correo certificado, será necesario que adicionalmente se envíe dentro de los tres días hábiles siguientes, mediante un mensaje de datos, la guía que compruebe que el referido documento fue depositado en una oficina de correos;
III. Que la información contenida en el documento electrónico se mantenga integra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta;
IV. Que el documento electrónico permita conservar el formato del documento impreso y reproducirlo con exactitud, y
V. Que se observe lo previsto en las disposiciones generales en materia de conservación de mensajes de datos y de los documentos electrónicos con firma electrónica avanzada.
Lo establecido en este artículo se aplicará sin perjuicio de que las dependencias y entidades observen, conforme a la naturaleza de la información contenida en el documento impreso de que se trate, los plazos de conservación previstos en los ordenamientos aplicables.

Datos Relevantes:

El título segundo, en su primer capítulo denominado "Del *uso y validez de la firma electrónica avanzada"*, se hace referencia en qué momento se podrá hacer uso de la firma electrónica, como lo es en documentos electrónicos y en mensajes de datos, especificando que producirán los mismos efectos jurídicos que una firma autógrafa. Posteriormente se presenta una serie de principios rectores que darán certeza y seguridad a la ley de la firma electrónica avanzada, siendo éstos: la equivalencia funcional, autenticidad, integridad, neutralidad tecnológica, no repudio y confidencialidad.

Cabe mencionar que señala que para que los sujetos puedan hacer un cabal uso de la firma electrónica, es necesario contar con un certificado digital vigente y homologado, así como una clave privada, la cual que se genera bajo el control de éstos.

Siguiendo con el articulado, en el capítulo dos, titulado *"De los documentos electrónicos y de los mensajes de datos"*, se especifica que las dependencias y entidades harán el uso de mensajes de datos y también deberán aceptar los documentos electrónicos con la firma electrónica avanzada del servidor público facultado para ello.

También se señala la necesidad de realizar una consulta del tablero electrónico, aceptar notificaciones que emita la dependencia o entidad y las acciones a seguir en caso de que la dependencia o entidad se encuentran imposibilitados para consultar el tablero electrónico o abrir los documentos electrónicos. Se hace necesario de igual forma que cada sujeto cuente con una dirección de correo electrónico para llevar a cabo las actividades concernientes a los documentos que contengan la firma electrónica avanzada.

Un aspecto también importante es la cuestión de la administración y control de accesos y respondiendo a lo anterior el artículo 13 señala que esto será responsabilidad de cada dependencia y entidad, atendiendo principios como seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia.

Otro aspecto que toca este capítulo es lo correspondiente a la observancia de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, ya que es sabido que la información gubernamental debe ser de acceso libre y transparente a menos que esté catalogada como de información confidencial.

A la par de lo anterior, se estipulan las bases que deben seguirse en caso de que se requiera que un documento sea impreso y con firma autógrafa, sea presentado o conservado en su forma digital.

TITULO TERCERO
DEL CERTIFICADO DIGITAL
CAPITULO I
De la estructura y procedimientos del certificado digital

ARTÍCULO 17.- El certificado digital deberá contener lo siguiente:

I. Número de serie:
II. Autoridad certificadora que lo emitió;
III. Algoritmo de firma;
IV. Vigencia;
V. Nombre del titular del certificado digital;
VI. Dirección de correo electrónico del titular del certificado digital;
VII. Clave Única del Registro de Población (CURP) del titular del certificado digital;
VIII. Clave pública, y
IX. Los demás requisitos que, en su caso, se establezcan en las disposiciones generales que se emitan en términos de esta Ley.

ARTÍCULO 18.- La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria establecerán de manera conjunta, en términos de las disposiciones aplicables, los procedimientos para la obtención y registro de datos y elementos de identificación, emisión, renovación y revocación de certificados digitales, los cuales darán a conocer a través de sus respectivas páginas Web.

ARTÍCULO 19.- La vigencia del certificado digital será de cuatro años como máximo, la cual iniciará a partir del momento de su emisión y expirará el día y en la hora señalados en el mismo.

CAPITULO II

Derechos y obligaciones del titular del certificado digital

ARTÍCULO 20.- El titular de un certificado digital tendrá los derechos siguientes:

I. A ser informado por la autoridad certificadora que lo emita sobre:

a) Las características y condiciones precisas para la utilización del certificado digital, así como los límites de su uso;

b) Las características generales de los procedimientos para la generación y emisión del certificado digital y la creación de la clave privada, y La revocación del certificado digital;

II. A solicitar la modificación de datos y elementos del certificado digital, mediante la revocación de éste, cuando así convenga a sus intereses.

ARTÍCULO 21.- El titular de un certificado digital estará obligado a lo siguiente:

I. Hacer declaraciones veraces y completas en relación con los datos y documentos que proporcione para su identificación personal;

II. Custodiar adecuadamente sus datos de creación de firma y la clave privada vinculada con ellos, a fin de mantenerlos en secreto;

III. Solicitar a la autoridad certificadora la revocación de su certificado digital en caso de que la integridad o confidencialidad de sus datos de creación de firma o su frase de seguridad hayan sido comprometidos y presuma que su clave privada pudiera ser utilizada indebidamente, y

IV. Dar aviso a la autoridad certificadora respectiva de cualquier modificación de los datos que haya proporcionado para su identificación personal, a fin de que ésta incorpore las modificaciones en los registros correspondientes y emita un nuevo certificado digital.

CAPÍTULO III

De las Autoridades Certificadoras

ARTÍCULO 22.- La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria son consideradas autoridades certificadoras para emitir certificados digitales en términos de esta Ley.

ARTÍCULO 23.- Las dependencias y entidades, distintas a las mencionadas en el artículo anterior, así como los prestadores de servicios de certificación que estén interesados en tener el carácter de autoridad certificadora en términos de la presente Ley, deberán:

I. Contar con el dictamen favorable de la Secretaría, y

II. Cumplir con los demás requisitos que se establezcan en las disposiciones generales que se emitan en los términos de esta Ley.

ARTÍCULO 24.- Las autoridades certificadoras tendrán las atribuciones siguientes:

I. Emitir, administrar y registrar certificados digitales, así como prestar servicios relacionados con la firma electrónica avanzada;

II. Llevar un registro de los certificados digitales que emitan y de los que revoquen, así como proveer los servicios de consulta a los interesados;

III. Adoptar las medidas necesarias para evitar falsificación, alteración o uso indebido de certificados digitales, así como de de los servicios relacionados con la firma electrónica avanzada;

IV. Mantener mecanismos que garanticen la confiabilidad de la firma electrónica avanzada, así como de los servicios relacionados con ésta;

V. Revocar los certificados de firma electrónica avanzada, cuando se actualice alguno de los supuestos previstos en el Reglamento y conforme a los procedimientos señalados en el artículo 18 de esta Ley;

VI. Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada, así como de los servicios relacionados con la misma, y

VII. Las demás que les confieran las disposiciones jurídicas aplicables.

Lo anterior, sin perjuicio de las atribuciones que, en su carácter de autoridad certificadora, corresponden al Servicio de Administración Tributaria en términos de la legislación fiscal y aduanera.

ARTÍCULO 25.- Las autoridades certificadoras tendrán la obligación de preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables.

ARTÍCULO 26.- Las autoridades certificadoras que sean reconocidas como tales en términos del artículo 23 de esta Ley, podrán dejar de tener ese carácter cuando se ubiquen en alguno de los supuestos previstos en el Reglamento de esta Ley.

ARTÍCULO 27.- La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria podrán coordinarse para acordar y definir, los estándares, características y requerimientos tecnológicos a que se deberán sujetar las autoridades calificadoras referidas en el artículo 23 de esta Ley, para garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada.

CAPÍTULO IV

Del reconocimiento de certificados digitales y de la celebración de bases de colaboración y convenios de colaboración o coordinación

ARTÍCULO 28.- La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria y demás autoridades certificadoras a que se refiere el artículo 23 podrán celebrar bases relacionadas con la firma electrónica avanzada.

ARTÍCULO 29.- El Ejecutivo Federal, por conducto de la Secretaría, de la Secretaría de Economía o el Servicio de Administración Tributaria, a solicitud de cualquier autoridad certificadora, podrán suscribir previa opinión de las otras dos, convenios de coordinación para el reconocimiento de certificados digitales homologados en términos de lo previsto en esta Ley, con:

I. Los poderes Legislativo y Judicial, federales;
II. Los órganos constitucionales autónomos, y
III. Los gobiernos de las entidades federativas, los municipios y los órganos político-administrativos del Distrito Federal.

Los convenios de coordinación que se suscriban deberán darse a conocer a las demás autoridades certificadoras, a través de la página Web de la Secretaría.

ARTÍCULO 30.- Los certificados digitales expedidos fuera de la República Mexicana tendrán las misma validez y producirán los mismos efectos jurídicos reconocidos en la presente Ley, siempre y cuando tales certificados sean reconocidos por las autoridades certificadoras a que se refiere el artículo 22 de la propia Ley que garantice, en la misma forma que lo que hace con sus propios certificados, el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado.

Datos Relevantes:

El título Tercero, en su capítulo III *"Derechos y obligaciones del titular del certificado digital"* aborda la cuestión referente a la estructura y procedimientos del certificado digital, resaltando que debe contener este certificado, como: número de serie, nombre de la autoridad certificadora que lo emitió, algoritmo de la firma, vigencia, nombre del titular del certificado digital, dirección de correo electrónico del titular del

certificado digital, Clave Única del Registro de Población (CURP), clave pública y demás requisitos que pudieses adherirse. La vigencia del certificado será de cuatro años.

En el capítulo II *"Derechos y obligaciones del titular del certificado digital*", **s**e establecen los derechos y obligaciones del titular del certificado digital, entre los derechos se destacan: el ser informado por la autoridad certificadora sobre características y condiciones para utilizar el certificado digital, características generales para la generación y emisión del certificado digital, a solicitar alguna modificación del certificado.

Entre las obligaciones tenemos que: el titular estará obligado a hacer declaraciones en relación a los datos y documentos que proporcione para su identificación personal, cuidar sus datos de creación de firma y clave privada, pedir a la autoridad certificadora la revocación de su certificado en caso que su clave sea utilizada indebidamente.

En el capítulo III *"De las Autoridades Certificadoras",* respecto a las autoridades certificadoras, se señala que éstas serán la Secretaría de la Función Pública, la Secretaría de Economía y el Servicio de Administración Tributaria y en caso de que otras dependencias y entidades estén interesadas en tener este carácter deberán ser avaladas por las anteriores. Se especifican las atribuciones de las autoridades certificadoras y un aspecto importante y digno de resaltar es la responsabilidad de garantizar la autenticidad, integridad conservación confiabilidad de la firma electrónica avanzada, así como los servicios relacionados con la misma.

En el capítulo IV "Del reconocimiento de certificados digitales y de la celebración de bases de colaboración y convenios de colaboración o coordinación", se habla del reconocimiento de certificados digitales y de la celebración de bases de colaboración y convenios de colaboración o coordinación; Especificándose que el Ejecutivo Federal, por conducto de las secretarías certificadoras podrán realizar estos convenios de coordinación con: los Poderes Legislativo y Judicial Federales, los órganos constitucionales autónomos y los gobiernos de las entidades federativas, los municipios y los órganos político administrativos del Distrito Federal.

Se establece que los certificados digitales expedido fuera de la República Mexicana tendrán la misma validez y producirán los mismos efectos jurídicos reconocidos en la presente Ley.

TITULO CUARTO
DE LAS RESPONSABILIDADES Y SANCIONES
CAPÍTULO ÚNICO

ARTÍCULO 31.- Las conductas de los servidores públicos que impliquen el incumplimiento a los preceptos establecidos en la presente Ley, dará lugar al procedimiento y a las sanciones que correspondan en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Cuando las infracciones a la presente Ley impliquen la posible comisión de una conducta sancionada en los términos de la legislación civil, penal o de cualquier otra naturaleza, las dependencias y entidades lo harán del conocimiento de las autoridades competentes.

Datos Relevantes:

Finalmente el título cuarto hace referencia a las responsabilidades y sanciones, se especifica que cualquier violación a esta Ley que implique el incumplimiento de algún precepto será sancionado en los términos que establezca la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos o de ser requerido, bajo la legislación civil, penal o de cualquier otra índole.

TRANSITORIOS

PRIMERO.- La presente Ley entrará en vigor a los 120 días hábiles siguientes al de su publicación en el Diario Oficial de la Federación.

SEGUNDO.- Se derogan todas aquellas disposiciones legales y administrativas que se opongan a los previsto en esta Ley.

TERCERO.- El Ejecutivo Federal expedirá el Reglamento de la presente Ley.

CUARTO.- Los certificados digitales expedidos con anterioridad a la entrada en vigor de esta Ley por los prestadores de servicios de certificación que, conforme a las disposiciones jurídicas aplicables, tangan reconocida la calidad de autoridad certificadora, así como por la Secretaría, la Secretaría de Economía y el Servicio de Administración.

DERECHO COMPARADO.

- **Cuadro comparativo de la denominación de la legislación en otros países**

PAÍS	DENOMINACIÓN DE LA LEGISLACIÓN
Argentina	Firma Digital: Ley 25.506[6]
Chile	Ley Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma: Ley N°19.799[7]
España	Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.[8]
Perú	Ley de Firmas y Certificados Digitales del Perú.[9]
Venezuela	Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas: Decreto N° 1.204.[10]

[6] **Argentina.** Legislación tomada de la Dirección Web:
http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
[7] **Chile.** Legislación tomada de la Dirección Web:
http://repositorio.idiem.cl/ley19799.pdf
[8] **España.** Legislación tomada de la Dirección Web:
http://www.csn.es/images/stories/documentos_adjuntos/oficina_virtual/legislacion/RDEC14_1999.pdf
[9] **Perú.** Legislación tomada de la Dirección Web.
http://www.policiainformatica.gob.pe/pdf/ley27269.pdf
[10] **Venezuela.** Legislación tomada de la Dirección Web:
http://www.tsj.gov.ve/legislacion/dmdfe.htm

CUADRO COMPARATIVO DE LA ESTRUCTURA (INDICE) DE LEGISLACIONES EN MATERIA DE FIRMA ELECTRÓNICA DE DIVERSOSO PAÍSES.

PAÍSES QUE CUENTAN CON LEGISLACIÓN EN MATERIA DE FIRMA ELECTRÓNICA	
ARGENTINA	**CHILE**
FIRMA DIGITAL **Ley 25.506**	LEY SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACION DE DICHA FIRMA N°19.799 Publicada en el Diario Oficial el 12 de abril de 2002
LEY DE FIRMA DIGITAL CAPITULO I Consideraciones generales CAPITULO II De los certificados digitales CAPITULO III Del certificador licenciado CAPITULO IV Del titular de un certificado digital CAPITULO V De la organización institucional CAPITULO VI De la autoridad de aplicación CAPITULO VII Del sistema de auditoría CAPITULO VIII De la Comisión Asesora para la Infraestructura de Firma Digital CAPITULO IX Responsabilidad CAPITULO X Sanciones CAPITULO XI Disposiciones Complementarias	TITULO I Disposiciones Generales TITULO II Uso de Firmas Electrónicas por los Órganos del Estado TITULO III De los Prestadores de Servicios de Certificación TITULO IV De los Certificados de Firma Electrónica TITULO V De la Acreditación e Inspección de los Prestadores de Servicios de Certificación TITULO VI Derechos y Obligaciones de los Usuarios de Firmas Electrónicas TITULO VII Reglamentos Tribunal Constitucional Proyecto de ley sobre firma electrónica y los servicios de certificación de firma electrónica.

ESPAÑA	PERÚ
Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.	**Ley de Firmas y Certificados Digitales del Perú**
TÍTULO I. DISPOSICIONES GENERALES CAPÍTULO ÚNICO. Disposiciones Generales. TÍTULO II. LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN. CAPÍTULO I. Principios Generales. CAPÍTULO II. Certificados. CAPÍTULO III. Condiciones exigibles a los Prestadores de Servicios de Certificación. CAPÍTULO IV. Inspección y Control de la Actividad de los Prestadores de Servicios de Certificación. 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. TÍTULO IV. TASA POR EL RECONOCIMIENTO DE ACREDITACIONES Y CERTIFICACIONES. CAPÍTULO ÚNICO. Tasa por el Reconocimiento de Acreditaciones y Certificaciones. TÍTULO V. INFRACCIONES Y SANCIONES. CAPÍTULO ÚNICO. Infracciones y Sanciones.	De la Firma Digital Del Titular de la Firma Digital De los Certificados Digitales De las entidades de certificación y de registro Disposiciones complementarias, transitorias y finales.

VENEZUELA
Decreto N° 1.204 10 de febrero de 2001 DECRETO CON FUERZA DE LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS
CAPITULO I AMBITO DE APLICACION Y DEFINICIONES Objeto y Aplicabilidad del Decreto –Ley Definiciones Adaptabilidad del Decreto-Ley CAPITULO II DE LOS MENSAJES DE DATOS Eficacia Probatoria Sometimiento a la Constitución y a la Ley Cumplimiento De Solemnidades Y Formalidades Integridad del Mensaje de Datos Constancia por escrito del Mensaje De Datos CAPITULO III DE LA EMISION Y RECEPCION DE LOS MENSAJES DE DATOS Verificación de la Emisión del Mensaje de Datos Oportunidad de la Emisión Reglas para la determinación de la Recepción Lugar de Emisión y Recepción Del Acuse de Recibo Mecanismos y Métodos para el Acuse de Recibo Oferta y Aceptación en los Contratos CAPITULO IV DE LAS FIRMAS ELECTRONICAS Validez y Eficacia de la Firma Electrónica. Requisitos Efectos Jurídicos. Sana Crítica La Certificación Obligaciones del Signatario CAPITULO V DE LA SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACION ELECTRONICA Creación de la Superintendencia Objeto de la Superintendencia Competencias de la Superintendencia Ingresos de la Superintendencia De las Tasas Mecanismos de Control De la Supervisión Medidas para garantizar la Confiabilidad

Datos Relevantes:

Respecto a los encabezados de los títulos y/o capítulos correspondientes a la legislación en cada uno de los países estudiados tenemos que algunos aspectos que abordar:

- Las Leyes de los cinco países cuentan con una parte correspondiente referente a "De los certificados digitales" el cual resulta ser un aspecto muy importante ya que permite tener una mayor certeza y seguridad de que no se está haciendo un mal uso de la información y de los datos.

- Desde esta perspectiva se considera que algunos de los puntos que se considera necesario poner atención o se destacan como más importantes[11] que algunos países abordan y otros no se destacan subrayados en el índice de cada país.

- Cabe mencionar que sin duda es necesario prestar especial atención al tema correspondiente a los organismos y/o entidades relacionados con la inspección y/o control de la firma electrónica, ya que en sus responsabilidades radica la importancia, seguridad y el adecuado funcionamiento de esta Ley.

[11] La parte que se destaca viene subrayada en los cuadros correspondientes a los índices de las legislaciones de cada país y posteriormente vienen desarrolladas por país para que sea más fácil el acceso a la legislación.

ASPECTOS QUE SE CONSIDERAN IMPORTANTES DE DESTACAR, POR PAÍS.

ARGENTINA

La legislación de este país en su Capítulo III titulado *"Del certificador licenciado"* define primeramente este concepto para otorgar una mayor claridad y entendimiento.

- 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.

Siguiendo esta línea también se expone quienes serán los 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.

Respecto a las funciones del certificador licenciado por destacarse algunas tenemos recibir la solicitud de emisión del certificado digital, emitir certificados digitales, mantener copia de todos los certificados digitales emitidos, informar públicamente el estado de los certificados digitales por él emitidos entre otras funciones.

En cuanto a las obligaciones del certificador licenciado mencionamos algunas, ya que por la amplitud del documento resulta necesario solo la descripción de algunas como Informar al solicitante de un certificado las condiciones para la utilización del certificado digital, abstenerse de hacer un mal uso de los datos de los titulares de los certificados digitales por él emitidos, mantener la confidencialidad de toda la información e impedir su divulgación, mantener la documentación respaldada de los certificados emitidos por diez años a partir de su fecha de vencimiento o revocación, publicar información en internet o en la red de acceso público siempre y cuando la autoridad lo determine, informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia, permitir el acceso a la información de funcionarios autorizados, contar con personal capacitado para las tareas necesarias entre otras obligaciones.

Se especifican los casos en los cuales el certificador licenciado cesa en tal calidad: decisión unilateral comunicada al ente licenciante, cancelación de su personería jurídica o por cancelación de su licencia dispuesta por el ente licenciante. Asimismo, se estipula en qué momento un certificado digital ya no será válido como al ser utilizado para alguna finalidad diferente a los fines para los cuales fue extendido,

para operaciones que superen el valor máximo autorizado cuando corresponda y una vez revocado.

El capítulo VII titulado "Del sistema de auditoría" expresa que tanto el ente licenciante y los certificadores licenciados deberán ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación. Asimismo, se describen los requisitos de habilitación de terceros para realizar estas auditorías.

El Capítulo VIII titulado "De la Comisión Asesora para la Infraestructura de Firma Digital" señala el cómo será integrada y cómo será el funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital, los cuales serán máximo 7 personas y estarán en su cargo 5 años, teniendo reuniones trimestrales.

CHILE

La Legislación en cuanto a la firma electrónica de este país establece en su Título II titulado "Uso de Firmas Electrónicas por los Órganos del Estado" establece que:

- 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.

Posteriormente se acredita que

- Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán validados de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel

Se indica el derecho de las personas a relacionarse con los órganos del Estado, a través de técnicas y medios electrónicos con firma electrónica, siempre que se ajusten a la Ley.

El título V de la ley titulado "De la Acreditación e Inspección de los Prestadores de Servicios de Certificación" estipula que:

- 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.

El prestador para ser acreditado debe tomar en cuenta entre algunos aspectos: demostrar la fiabilidad necesaria de sus servicios, garantizar la existencia de un

servicio seguro de consulta del registro de certificados emitidos así como emplear personal capacitado para la prestación de los servicios ofrecidos, contar con capacidad tecnológica necesaria para el desarrollo de la actividad de certificación entre otros.

En el Título VI titulado "Derechos y Obligaciones de los Usuarios de Firmas Electrónicas" se expresa que entre otros derechos los usuarios o titulares de firmas electrónicas deben ser informados por el prestador de servicios de certificación, de las características generales de los procedimientos de creación y verificación de firma electrónica, a que su información sea confidencial, a ser informado antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, a ser informado de la cancelación en la inscripción en el registro de prestadores acreditados, a traspasar sus datos a otro prestador de servicios de certificación entre otros derechos.

ESPAÑA

Cabe destacar antes de otorgar los datos relevantes que España es sin duda uno de los países pioneros en la incorporación a su legislación de esta Ley por tanto, se considera necesario que este país la revise nuevamente y haga las modificaciones necesarias, ya que debido a los cambios tan vertiginosos y el avance de las comunicaciones resulta necesario tener una legislación acorde al tiempo actual.

El Capítulo III titulado "Condiciones exigibles a los prestadores de servicios de certificación" tenemos las obligaciones de los prestadores de servicios de certificación:

Obligaciones de los prestadores de servicios de certificación.

- Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.
- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.
- Mantener un registro de certificados, en el que 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.
- 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.

- Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación y Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-Ley y en sus normas de desarrollo.

Debe insistirse en que esta legislación también cuanta con otro apartado titulado: **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 % 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 %.

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 estén disponibles para verificación de firmas electrónicas.
2. 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.

Respecto al cese de la actividad tenemos el prestador de servicios de certificación que vaya a cesar su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos.

Respecto a la responsabilidad de los prestadores de servicios de certificación se estipula que 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 dicha ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.

Otro aspecto de suma importancia es la cuestión relacionada a la inspección y control y atendiendo este criterio el Capítulo IV titulado “Inspección y control de la actividad de los prestadores de servicios de certificación” estipula que:

- 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.

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

- Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, 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.

PERÚ

De esta Ley, lo que resulta desde este punto de vista destacar es el apartado titulado De las entidades de certificación y registro. En cuanto a la Entidad de Certificación tenemos que:

- 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.

Y en cuando a la Entidad de Registro o Verificación tenemos que:

- 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.

Un aspecto innovador que esta Ley contiene y que hasta el momento no se ha encontrado en las demás legislaciones estudiada es que cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado. Cabe decir que la información al igual que las otras legislaciones tendrá el carácter de confidencial a menos que exista una solicitud para accesar por medios telemáticos tomando las indicaciones necesarias.

VENEZUELA

Los Capítulos IV, V y VI de la Ley de Venezuela que atienden cuestiones relacionadas con la validez, eficacia, superientendencia, certificación, proveedores de servicios de servicios de certificación y mecanismo de control de la firma electrónica resultan ser los más acordes a abordar. Del Capítulo IV titulado "*De las firmas Electrónicas: Validez y Eficacia de la Firma Electrónica. Requisitos"* lo más relevante por señalar radica en que la Firma Electrónica:

- Permite vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa.

Los aspectos que la Firma Electrónica debe llenar son:

1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
3. No alterar la integridad del Mensaje de Datos.

A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

El Capítulo V titulado "De la superintendencia de servicios de certificación electrónica" tenemos que existe un articulado que nos habla sobre la creación de una superintendencia la cual será creada como:

- Un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Aunado a lo anterior tendrá por objeto acreditar, supervisar y controlar y para lograr esto a continuación se enumeran las **Competencias de la Superintendencia de Servicios de Certificación Electrónica:**

1. Otorgar la acreditación y la correspondiente renovación a los Proveedores de Servicios de Certificación una vez cumplidas las formalidades y requisitos de este Decreto-Ley, sus reglamentos y demás normas aplicables.
2. Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.
3. Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados.
4. Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.
5. Supervisar las actividades de los Proveedores de Servicios de Certificación conforme a este Decreto-Ley, sus reglamentos y las normas y procedimientos que establezca la Superintendencia en el cumplimiento de sus funciones.

6. Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.
7. Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.
8. Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.
9. Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.
10. Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.
11. Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.
12. Requerir de los Proveedores de Servicios de Certificación o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.
13. Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificados y sus usuarios, cuando ello sea solicitado por las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige esta materia.
14. Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.
15. Presentar un informe anual sobre su gestión al Ministerio de adscripción.
16. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.
17. Imponer las sanciones establecidas en este Decreto-Ley.
18. Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.
19. Las demás que establezcan la ley y los reglamentos.

En cuanto a **Mecanismos de control** tenemos que la Contraloría Interna del Ministerio de Ciencia y Tecnología, ejercerá las funciones de control, vigilancia y fiscalización de los ingresos, gastos y bienes públicos sobre este .servicio autónomo, de conformidad con la ley que regula la materia.

Y en cuanto a **Supervisión** se establece que la Superintendencia de Servicios de Certificación Electrónica supervisará a los Proveedores de Servicios de Certificación con el objeto de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz a sus usuarios. A tal efecto, podrá directamente o a través de expertos, realizar las inspecciones y auditorias que fueren necesarias para comprobar que los Proveedores de Servicios de Certificación cumplen con tales requerimientos.

Finalmente el Capítulo VI hace referencia a los requisitos para ser proveedor y se refieren relativamente a los aspectos mencionados en las anteriores legislaciones.

OPINIONES ESPECIALIZADAS.

Este como muchos temas de interés y trascendencia jurídica, han sido retomados por distintos expertos en la materia para emitir distintos análisis y criterios, ya sea técnicos y/o jurídicos, entre los cueles se muestran a continuación algunos de ellos:

[12] **"Debate y análisis del uso e impacto de la firma electrónica en México Nuestra "llave" digital**

"…
Si la firma cumple 3 funciones exigidas en la normativa (identificación de las partes, autenticación del contenido e integridad del contenido) y puede asimismo cumplir las funciones de confidencialidad del mensaje y de no repudio en origen y en destino, la parte de identificación es absolutamente vital en tanto en cuanto constituye el primer paso de la cadena de confianza.
Si no se identifica de manera absolutamente fehaciente al titular de la firma electrónica, al signatario poseedor de los datos de creación de firma, todo lo demás está viciado. Y ¿cómo se identifica al usuario? En la mayoría de los casos, mediante datos personales. De ahí que considere que es esencial conocer a cabalidad la regulación que impera sobre el tratamiento y gestión de dichos datos.
Ya he dicho en muchas ocasiones, quizá alguno piense que hasta demasiadas, que la firma electrónica constituye nuestra identidad digital.Y esa identidad digital sólo está conformada por datos. Datos que unidos a nuestra persona conforman la información personal.
Hoy leo en la prensa que las autoridades se han puesto en marcha para recabar las voces de reos en México, intentando crear un registro lo más amplio posible que recabe dichas voces que luego se puedan contrastar con los registros de grabaciones provenientes de delitos como la extorsión.
Por supuesto, si atendemos al concepto de dato personal, la voz es claramente una información concerniente a una persona física que le hace identificada o identificable. Precisamente ése es el objetivo del registro, identificar a un presunto delincuente. De ahí que, de nuevo, vamos viendo cada vez más pasos hacia la constitución de una persona con una identidad "paralela" a la física.
…
…
Firma electrónica no es sólo el mecanismo que nos darán para hacer nuestras transacciones en línea, con el Sector Privado o con la Administración, sino que constituye nuestra identidad, nuestra persona, digital. Puede parecer exagerado, pero más bien yo creo que los ejemplos que poco a poco vamos viendo cada día nos dan una idea de que tenemos que aprender a cuidar a nuestro ser en el entorno electrónico tanto o más como acostumbramos en el mundo real. A veces hasta dudo cuál es más real, al

[12] "Debate y análisis del uso e impacto de la firma electrónica en México Nuestra "llave" digital". Nota tomada de Blogs de Política Digital, Innovación Gubernamental. Escrito por Isabel Davara el día jueves 6 de enero de 2011. Dirección Web: http://blogs.politicadigital.com.mx/firma-electronica/?p=328.

menos cuantitativamente, en función de las horas que pasamos en uno u otro, en nuestras vidas".

España es uno de los países pioneros en abordar este asunto de la firma electrónica a través de la implementación de diversos ordenamientos en la materia, es por ello que cuenta con distintos documentos de análisis al respecto, entre éstos se muestran los siguientes:

[13] "Firma Electrónica

RESUMEN
A medida que la informática se incorpora a más aspectos de la vida cotidiana, muchos trámites que tradicionalmente se realizaban en papel pasan a efectuarse de manera electrónica. Esto representa una ventaja para el tratamiento de la información.
Sin embargo, la propia naturaleza física del papel y la escritura ha sido utilizada también con ciertos fines. La dificultad de alterar un medio físico de representación de la información sirve como medida de seguridad contra las falsificaciones. La firma manuscrita, por otra parte, puede asociarse a su autor con un alto grado de certeza y sirve, por tanto, para acreditar su consentimiento, conocimiento o autorización en relación con la información escrita. Lógicamente, esto resulta fundamental en todo tipo de acuerdos, transacciones comerciales, etc.
Puede pensarse que los procedimientos electrónicos, en principio, no ofrecen estas posibilidades. En este documento se ofrece una somera introducción al funcionamiento de la firma electrónica y en qué medida permite que las transacciones electrónicas sustituyan a las manuscritas sin tener que renunciar a ninguna de sus ventajas.

CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA.
Antes de entrar en la aplicación específica a la firma electrónica, conviene conocer el fundamento de la misma: la criptografía de clave asimétrica.
Es conocido que cuando se transmite información el mensaje puede ser interceptado por terceros, que tendrían acceso a dicha información de forma no autorizada. Para evitarlo, se utiliza la encriptación. El emisor altera (de manera reversible) el mensaje original mediante el uso de una clave; el mensaje alterado (y por tanto ilegible) se transmite a salvo de intromisiones, y el receptor aplica la clave para devolver el mensaje a su estado original.
Este proceso plantea dos requisitos: uno, que sea imposible (a efectos prácticos) recuperar el mensaje original a partir del alterado si no se posee la clave. Otra, que el emisor y el receptor dispongan de la clave, pero el espía no.
Existen métodos de criptografía lo suficientemente avanzados que garantizan la imposibilidad práctica de *adivinar* la clave de cifrado. Pero existe un problema si la misma clave se utiliza para cifrar y para descifrar: si el emisor y el receptor no disponían de la clave de antemano (cosa habitual en transacciones electrónicas, en las que las partes nunca se han visto), tendrán que enviársela, y este envío compromete la seguridad.

[13]"Firma Electrónica". Agustín Cernuda del Río Universidad de Oviedo. Artículo tomado el día 06 de enero de 2011 de la Dirección Web: http://www.di.uniovi.es/~cernuda/pubs/comercio2002.pdf.

Los métodos de criptografía de clave asimétrica se basan en el uso de dos claves. Ambas sirven para cifrar y para descifrar, pero lo que se cifra con una sólo se puede descifrar con la otra, y viceversa. De este modo, una persona dispone de dos claves; una de ellas será pública, y la otra privada. Cualquiera que desee enviarle un mensaje confidencial puede usar la clave pública para cifrarlo; de este modo el mensaje viajará seguro, y el receptor utilizará su clave privada para descifrarlo. No necesita darle su clave privada a nadie ni arriesgarse a que alguien la *escuche*; la clave pública, por su parte, permite a todo el mundo enviarle mensajes cifrados, pero es inútil para descifrarlos.

FUNDAMENTOS DE LA FIRMA ELECTRÓNICA.

¿Qué relación tiene el cifrado de mensajes con la firma electrónica? El problema de los documentos electrónicos es que, a priori, su falsificación resulta técnicamente más sencilla que en los documentos físicos. Puesto que un documento electrónico contiene únicamente información, no ligada a ningún soporte ni acción física concreta, la información podría alterarse sin dejar huella física alguna. Evidentemente, esto abre las puertas a muchos tipos de fraude: falsificación de mensajes y cartas, modificación maliciosa de las condiciones de los contratos, o suplantación de personalidad, por citar sólo algunos.

El cifrado puede utilizarse como elemento de apoyo para la firma electrónica. Lo que pretende la firma es, esencialmente, lo siguiente:

− Acreditar la validez de un documento, de modo que no pueda ser alterado o sustituido por otro.

− Vincular un documento a una persona o entidad.

La criptografía de clave asimétrica permite ambas cosas. Para *firmar* un documento, bastaría acompañarlo de una versión cifrada del mismo, que el firmante ha cifrado con su clave privada. Como ya se ha dicho, es imposible a efectos prácticos generar tal versión cifrada sin disponer de la clave, que el firmante conserva en su poder y no comunica a nadie. Además, los métodos de cifrado garantizan que cualquier mínima alteración en el documento original producirá una versión cifrada notablemente distinta.

El receptor puede tomar ambos documentos, el original y el cifrado (que es la *firma* que lo acompaña), y usando la clave pública del firmante (que es conocida por todos) descifrar dicha firma. Si el resultado coincide con el documento, efectivamente sabemos que este no ha sido alterado y además el firmante es quien dice ser, ya que sólo él tiene la clave privada y sólo con esa clave se puede haber cifrado el documento.

El método no es matemáticamente infalible. Por ejemplo, ¿cómo estar seguros de que la clave pública es la del firmante y nadie nos ha engañado? Para eso existen las llamadas autoridades de certificación, que son entidades que garantizan la asociación entre una persona física y su clave pública. En cualquier caso, aunque en teoría es posible la suplantación, la fiabilidad del método es suficiente para su uso práctico; al fin y al cabo, la firma manuscrita tampoco está a salvo de falsificaciones.

ASPECTOS LEGALES DE LA FIRMA ELECTRÓNICA

Los poderes públicos están promoviendo el desarrollo de la llamada *sociedad de la información* mediante diversos planes de actuación [1], y la firma electrónica resulta de gran importancia en la consecución de este objetivo. Una vez presentados los fundamentos técnicos que posibilitan la firma electrónica, cabe preguntarse por su uso práctico, así como por el valor legal de la firma electrónica.

Marco normativo

Existen diversos códigos legales que afectan al uso de la firma electrónica. Existe una Directiva Europea 1999/93/CE, del 13/12/1999 [2], que afecta a los países miembros de la Unión y debía aplicarse antes del 19 de julio de 2001; no obstante, España se adelantó a la promulgación de esta directiva con el Real Decreto-Ley 14/1999 sobre firma electrónica [3], promulgado el 17 de septiembre de 1999.

Posteriormente, se publicó el Reglamento de Acreditación en forma de Orden Ministerial [4], el 21 de febrero de 2000. Se aplica a los prestadores de servicios de certificación, es decir, a las entidades que ofrecen productos de firma electrónica y garantizan la asociación entre las claves y las personas.

Se pretendía tramitar el R.D.L. 14/1999 como Proyecto de Ley, a fin de que el debate parlamentario permitiera perfeccionarlo. No obstante, la legislatura terminó en marzo de 2000, por lo que se pospuso tal tramitación.

En 2002 surge una nueva iniciativa para perfeccionar algunos aspectos de la Ley, y se presentan sendos Borradores de Anteproyecto de Ley de Firma Electrónica, el primero en enero de 2002 y el segundo en julio [5]. Esa es la situación en el momento actual (noviembre de 2002).

Validez legal de la firma electrónica

La legislación vigente en España sigue las directrices de la norma europea ya mencionada. Básicamente, la denominada firma electrónica *avanzada* tiene para los documentos electrónicos la misma validez que la firma manuscrita para los documentos en papel. Por ello debe aceptarse como prueba en un juicio, y en caso de que el firmante alegue error o falsedad, el juez decidiría previa intervención de los peritos correspondientes. Es decir, lo mismo que se aplica a la firma manuscrita. Existe, además, una presunción de validez de la firma si el prestador de servicios de certificación implicado está *acreditado* (la ley detalla en qué consiste esta *acreditación*).

Existen otros tipos de firma electrónica, que al no cumplir todos los requisitos establecidos por la ley no se calificaría como *avanzada*. En el caso de la firma *simple* o *no avanzada*, la ley garantiza cuando menos que dicha firma no se rechazará de plano como prueba por el mero hecho de ser electrónica.

La firma electrónica no sustituye las funciones de los fedatarios públicos. Cuando un notario interviene en una escritura pública no sólo verifica la identidad de los firmantes, sino que también enjuicia su capacidad para contraer las obligaciones correspondientes, y la firma digital es inútil para esto.

…

CONCLUSIONES

La transición de la gestión física de la información a un modelo electrónico exigía medios de firma similares a los existentes tradicionalmente, a fin de garantizar la confidencialidad, autenticación, integridad y no repudio que se veían comprometidas en el ámbito digital. La criptografía de clave asimétrica ofreció una solución técnica sobre la cual puede edificarse un nuevo conjunto de relaciones electrónicas; para ello sólo se necesitaba un marco jurídico que ya está, en gran medida, desarrollado, y la difusión de la firma digital entre el gran público hasta el punto de convertirse en algo cotidiano, cosa que también parece que se logrará en un futuro cercano. El DNI electrónico puede ser un paso decisivo en esa dirección".

Una aportación más de la situación de aquel país, - la cual cabe señalar, nos ilustra de forma importante- es la siguiente:

[14] **"La Firma Electrónica: Mayor Seguridad en la Red**

Se proponen cambios en la regulación de la firma electrónica, para impulsar el comercio electrónico. La confianza y la seguridad de los usuarios es clave para conseguirlo. Pero, ¿sabe usted qué es exactamente y cómo funciona?
¿Qué es la firma electrónica?
La firma electrónica o digital es un conjunto de datos electrónicos que identifican a una persona en concreto. Suelen unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se tratara, de esta forma el receptor del mensaje está seguro de quién ha sido el emisor, así como que el mensaje no ha sido alterado o modificado.
La firma electrónica puede utilizarse en el sector privado, para contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo, la compra de un libro o un compacto por Internet) y entre empresas (por ejemplo, realizar un pedido a un distribuidor) o incluso entre los mismos consumidores finales (por ejemplo, venta de una raqueta de 2° mano, una colección de monedas etc).
También nos sirve para realizar actuaciones con y entre la Administración, es decir, sirve tanto para las relaciones entre los propios entes públicos que la forman como para las relaciones del ciudadano con la Administración (por ejemplo, algo tan simple como la renovación del D.N.I, la solicitud de prestaciones a la Seguridad Social o incluso la presentación de la declaración de la renta por Internet con el conocido programa "Padre").

¿Cómo funciona la firma electrónica?

La firma electrónica funciona mediante la encriptación o cifrado de los datos que la componen, de forma que si no se tiene la clave, el documento se convierte en ilegible. Para ello es necesario contar con un par de claves: clave privada y clave pública que se corresponden de forma matemática. Pongamos un ejemplo, escribimos un documento y lo firmamos con nuestra clave privada y lo enviamos a nuestro receptor al cual previamente le habremos otorgado nuestra clave pública, esta clave pública es la que permite verificar la procedencia del mensaje y que verdaderamente ha sido firmado por nosotros, que somos los únicos poseedores de la clave privada)
Con esta encriptación se consigue que:
- La información enviada bajo la firma electrónica sólo pueda leerse por la persona autorizada que posea la clave.
- Acreditar la identidad de quien firma el documento electrónicamente.
¿Cuántos tipos de firma electrónica existen?
En nuestra actual normativa existen dos tipos: la básica y la avanzada.

[14]La Firma Electrónica: Mayor Seguridad en la Red. Por María José Ruiz Lancina. Jurista. Licenciada en Derecho y Doctorando en el Departamento de Derecho de la Empresa de la Facultad de Derecho (Universidad de Zaragoza). Nota tomada el día miércoles 05 de enero de 2011 de la dirección Web: *http://www.informatica-juridica.com/trabajos/La_firma_electronica_mayor_seguridad_en_la_red.asp.*

La firma electrónica básica contiene un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio documento, pero este sistema tiene algunos problemas. ¿Cómo sabemos que los datos enviados hayan sido creados por la persona que lo firma o que verdaderamente lo ha firmado él y no una tercera persona haciéndose pasar por él?
Para resolver este problema se crea la firma electrónica avanzada, a la que nuestro ordenamiento atribuye plena eficacia jurídica y valor probatorio en juicio. Permite la identificación del emisor del mensaje ya que está vinculada de manera única al que firma el documento y a los datos que incorpora, debido a que es el signatario quien únicamente posee el control exclusivo de estas claves, además de que permite saber si estos datos han sido modificados posteriormente o en su transcurso.
Sin duda son figuras todavía desconocidas y complicadas para el uso y entendimiento de la población, no sólo porque son tratadas desde un punto de vista excesivamente técnico, sino por la propia ambigüedad que produce la lectura de las definiciones que ofrece la regulación actual.
¿Quién autentifica las firmas electrónicas?
Las autoridades de certificación, que son personas o entidades que cumplen una serie de requisitos legales y que deben ser autorizados por el Ministerio de Justicia para otorgar certificados que acrediten que la persona o entidad que usa dicha firma es ciertamente quien dice ser.
…
En España la prestación de estos servicios es libre, si bien existe un procedimiento voluntario, que es la acreditación, mediante la cual la Administración, realizando las evaluaciones técnicas de rigor, emite una resolución o documento oficial donde certifica que ese Prestador cumple con las normas de calidad y seguridad establecidas en cuanto a sus procedimientos y a los productos y tecnología que utiliza.
…".

Ya concretamente en el caso mexicano, y más en relación a la iniciativa presentada por el Ejecutivo en diciembre del 2010, distintos medios abordaron el tema, de la siguiente forma:

[15] "**Ley de Firma Electrónica**

El Ejecutivo federal mandó al Senado la iniciativa de Ley de Firma Electrónica Avanzada que busca, entre otros objetivos, frenar la corrupción y mejorar trámites y servicios públicos.
De acuerdo con un oficio de la Secretaría de Gobernación, se busca regular la firma electrónica para que a través de medios de comunicación electrónica se utilice por los servidores públicos y particulares en trámites, servicios y procedimientos administrativos de las dependencias y entidades de la Administración Pública Federal, de la PGR y las unidades administrativas de la Presidencia. Esto, de acuerdo con el documento, permitirá la mejora de trámites y servicios públicos, así como de los

[15]"Ley de Firma Electrónica". Carole Simonnet. Viernes, 10 de diciembre de 2010. Nota tomada el día 06 de enero de 2011 de la Dirección Web: *http://www.elmanana.com.mx/notas.asp?id=212353*

procedimientos administrativos y, consecuentemente, inhibir la práctica de actos de corrupción, reducir la discrecionalidad, incrementar la transparencia y hacer más eficiente la gestión gubernamental.

La iniciativa señala que la información contenida en los mensajes de datos y en los documentos electrónicos será pública salvo que se clasifique como reservada o relacionados con las materias fiscal, aduanera y financiera, con miras a mantener la estabilidad del sistema financiero, y en otros actos que determine la Secretaría de la Función Pública. Sin embargo, la iniciativa establece que el Servicio de Administración Tributaria actuará como autoridad certificadora para la expedición de certificados digitales.

La propuesta de Ley, que contiene cuatro títulos y 31 artículos, plantea establecer un certificado digital y una clave privada para regular su uso confidencial en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. La Función Pública será la encargada de apoyar la implementación de la firma electrónica.

El Ejecutivo explica que la dependencia ha emitido ya entre 2000 y a la fecha más de un millón de certificados de firma electrónica, sin embargo reconoce que no se ha logrado extender a toda la Administración. "No obstante las acciones y los esfuerzos que se han realizado en el ámbito de la Administración Pública Federal, a la fecha no se ha logrado el uso generalizado de la firma electrónica avanzada como una herramienta indispensable en el desarrollo de las actividades entre las instituciones públicas y entre éstas con los particulares", indica.

En la exposición de motivos se explica que en lo local, las legislaturas de los estados de Colima, Guanajuato, Hidalgo, Jalisco, Sonora, Yucatán y la Asamblea Legislativa del Gobierno del Distrito Federal han impulsado la aprobación de leyes especiales para reconocer el uso de la firma electrónica".

[16] "La Firma Electrónica y su futuro en México

Las transacciones electrónicas en México han encontrado el desarrollo de una regulación jurídica, el cual les otorga la seguridad necesaria para el impulso y perfeccionamiento de los negocios electrónicos en nuestro país.

Aunque de manera tardía, pero finalmente nuestro país se ha sumado al proceso de legalizar y darle viabilidad a la firma electrónica; sin embargo, ahora queda pendiente el desarrollo de la factura electrónica y su vinculación a la contabilidad.

El pasado 29 de agosto de 2003, se estableció el antecedente más importante en esta materia al marcar una actualización en la legislación mexicana en relación con la forma como las nuevas tecnologías han modificado el derecho mercantil y la interacción en la sociedad.

A pesar de las reformas que reconocen la validez jurídica de la firma electrónica, las empresas de nuestro país requerían de la motivación para cambiar la forma de hacer negocios y poner en práctica las nuevas tecnologías en su "portafolio" de estrategias de negocio; además, hacía falta un impulso en materia fiscal que permitiera llevar a la práctica conceptos plasmados en la ley mercantil, tales como: firma electrónica, certificado digital, contratos electrónicos, etc.

[16] "La Firma Electrónica y su futuro en México". Lic. Valentino Francisco Cornejo López. Nota tomada de de la Dirección Web: http://idup.gdl.up.mx/ficheros/firma.pdf.

En este sentido, el Sistema de Administración Tributaria (SAT) desarrolla la estructura y la función de la firma electrónica a través de Internet con el proyecto e-firm, mismo que se pondrá en operación en el año 2005; éste proporcionará un certificado digital, con el cual los contribuyentes tendrán la posibilidad de usar la tecnología electrónica para cumplir con sus obligaciones fiscales. Se prevé que la puesta en marcha del uso de los medios electrónicos facilite la realización del pago de impuestos; por ejemplo, al enviar las declaraciones fiscales o realizar consultas al SAT por parte de las personas morales.
Es claro que la política fiscal planteada por la Secretaría de Hacienda y Crédito Público (SHCP), está apostando a las nuevas tecnologías para reducir el índice de evasión fiscal, aumentar la recaudación y agilizar el intercambio de información; muestra de ello es que para el próximo año, el SAT se prepara para el funcionamiento de la factura electrónica y la posibilidad de llevar la contabilidad a través de los sistemas digitales, utilizando en estos procesos la firma electrónica basada en criptografía asimétrica y el uso de la llave pública y privada.
En un estudio de Gartner, se muestra que los costos de operación descienden a 50%, pues la utilización de la factura tradicional conlleva un gasto de 80 centavos de dólar estadounidense, frente a 35 centavos que implica el uso de comprobantes fiscales electrónicos.
A pesar de las reformas en los códigos civiles, procesales, de comercio, fiscal y la realización de los diferentes proyectos por parte del gobierno, prevalece una incertidumbre al omitir de las regulaciones una figura como la firma electrónica avanzada única para todas las operaciones, no sólo las tributarias. Hasta ahora, la firma electrónica avanzada es empleada por: la SHCP; la Secretaría de la Función Pública la esgrime para efectuar las declaraciones patrimoniales de los
funcionarios de la Administración Pública Federal; por su parte los Registros Públicos de la Propiedad y del Comercio la operan con el propósito de que sus empleados capturen información en el programa de cómputo de gestión de registros públicos (SIGER); además, las dependencias de la Administración Pública y los notarios públicos y corredores públicos pueden emitir certificados de firmas electrónicas, principalmente de aquéllas empleadas en el extranjero.
En cuanto al proceso de certificación que se llevará a cabo ante el SAT, es importante resaltar la participación y responsabilidad de los altos mandos de las empresas en los trámites fiscales a través de medios electrónicos, pues el proceso de certificación requiere de la comparecencia de los representantes legales que cuenten con facultades para realizar actos de administración o de dominio de las empresas a las cuales representan, mismas que no deben ser tomadas a la ligera, ya que este tipo de apoderados será el único que podrá presentar declaraciones o promociones; también en el proceso de emisión de facturas electrónicas serán ellos quienes podrán obtener los sellos digitales que hace las veces de firma electrónica para su empleo en las facturas.
Una de las ventajas del uso de la firma electrónica en las facturas es que impide la violación o alteración de los datos, en particular del sello digital, puesto que se encuentra protegido por mecanismos criptográficos, es decir, una serie de procesos matemáticos que garantizan la fiabilidad y la seguridad de los datos. Al recibir una factura electrónica, el cliente podrá reconocer su validez mediante un proceso de autenticación que deberá tener desarrollado; así, sabrá si el documento es auténtico o tuvo alteraciones, o si la firma corresponde o no al emisor.
Se prevé que en el lapso de cinco años aproximadamente, el sector empresarial emitirá facturas electrónicas, debido a que será una obligación fiscal; sin embargo, es necesario

considerar que se trata de una modificación sustancial de los procesos de negocio, dada la incidencia de la relación costo-beneficio.
Por ello, las empresas deberán cumplir con los requisitos y procedimientos establecidos por el Banco de México, el SAT, la Secretaría de Economía y cuidar su perfecta operación desde el punto de vista fiscal, legal y tecnológico; de no hacerlo, se estarían incumpliendo las obligaciones fiscales, con la consecuente responsabilidad legal, contractual, entre otras.
Por último, cabe destacar que la responsabilidad de expedir facturas fiscales electrónicas por la inclusión del sello digital, es idéntica a la de la firma electrónica avanzada, esto es, tendrá las mismas consecuencias jurídicas por el uso de la firma electrónica, incluso penales, del titular del certificado que ampara la firma electrónica".

[17] **"Presentan Iniciativa de Ley de Firma Electrónica Avanzada; regula su uso en trámites administrativos vía internet; no aplica en casos fiscal, aduanero y financiero**

El presidente Felipe Calderón envió ayer al Senado la iniciativa de Ley de Firma Electrónica Avanzada, cuya finalidad es reducir los costos de transacción relacionados con el comercio y los trámites y servicios que los ciudadanos llevan a cabo como personas físicas o morales. La firma electrónica como lo explicó la dependencia permitirá al ciudadano realizar trámites y transacciones a cualquier hora y desde cualquier parte con acceso a internet, así como transacciones electrónicas vía Web bajo un ambiente de seguridad jurídica y confiabilidad. El proyecto de ley presidencial fue recibido ayer mismo por la Cámara Alta.
La Firma Electrónica Avanzada asegurará la autenticidad de los datos, evitará el repudio en envío de los mismos, permitirá mantener la integridad de los documentos al restringir modificaciones a los mensajes y asegurará la confidencialidad al restringir el acceso o la distribución no autorizada de mensajes, datos y documentos electrónicos.
La información que incluye la firma electrónica avanzada es equiparable a los documentos impresos con firma autógrafa y producirá los mismos efectos jurídicos que las leyes otorgan a estos documentos. Es decir que en todos los actos jurídicos ya sean comunicaciones, procedimientos administrativos, trámites y servicios o transacciones comerciales llevados a cabo con la firma digital tendrán pleno valor probatorio y de identificación de la persona que los realiza.
La Firma Electrónica Avanzada y su pleno reconocimiento con la iniciativa de ley presentada por el presidente Felipe Calderón facilitará el comercio nacional e internacional y favorecerá la competitividad de las empresas mexicanas, pues su uso fomentará las operaciones seguras entre particulares. Además la firma digital optimizará el aprovechamiento de tecnologías de la información y comunicaciones, a través de la sistematización y digitalización de todos los trámites administrativos para la gestión pública para brindar una mejor y más rápida atención a los ciudadanos.
Su uso explicó la SFP incidirá en una mayor eficiencia en la gestión gubernamental, la transparencia y en la generación de ahorros, ante la reducción de tiempos, recursos humanos y económicos del sector público y de los ciudadanos.

[17] Presentan Iniciativa de Ley de Firma Electrónica Avanzada; regula su uso en trámites administrativos vía internet; no aplica en casos fiscal, aduanero y financiero". Redacción del periódico la Nota tomada el día miércoles, 05 de enero de 2011 de la Dirección Web: *http://www.cronica.com.mx/nota.php?id_nota=549176*

De acuerdo con la iniciativa, las autoridades certificadoras de firmas digitales serán la Secretaría de Economía (SE), el Servicio de Administración Tributaria (SAT) y la Secretaría de la Función Pública (SFP)".

[18] **"Lo bueno, lo malo y la fea…(tercera y última)**

Ya lo pensó?. ….decidió obtener su Firma Electrónica Avanzada, entonces deberá de acudir a un ente Certificador para emitirle su Certificado Digital, el cual prueba que usted cuenta con una FEA y que los documentos que usted firma a través de medios electrónicos con su FEA son emitidos precisamente por usted y no por nadie más.
Ahora que podemos sacar de todo esto, me refiero a algo bueno por supuesto. Primeramente podemos aprovechar el que ya contamos con un Certificado Digital y quizá alguna contraparte en relaciones contractuales también cuente con dicho Certificado, de ser así, podrán acordar algún procedimiento de envío y recepción de datos a través de medios electrónicos (correo electrónico) que les permita llevar una relación comercial y de negocios completamente confiable.
Lo anterior significa que establecido esto, se pueden hacer pedidos, apartados, contrataciones de servicios de cualquier índole, en el entendido de que quien hace el requerimiento es sin duda el autorizado por parte de la empresa contratante para obligar a esta en esa relación, aunado a que la contraparte es igualmente la persona idónea para obligar o aceptara compromisos respecto del servicio o acto comercial que se este contratando.
No por nada el comercio electrónico se ha regulado y normado a través del Código de Comercio, permitiendo así que existan reglas los suficientemente claras como para crear los procesos que sean lo suficientemente seguros como para, incluso, en juicio tener pruebas plenas de la relación y de la firma de los compromisos como si se hubiera hecho en forma autógrafa.
Ahora bien si usted considera poco viable obtener su FEA a través de entes públicos, como puede ser la Secretaría de Hacienda o el SAT, aun así puede generar comercio electrónico sobre las bases que regula el Código de Comercio, pues existen otro entres certificadores que emiten los Certificados Digitales y que tienen por resultado generar una dinámica comercial muy atractiva.
Los pasos debe de seguir usted para ello son: primero acudir a un prestador de servicios de certificación, para obtener su Firma Electrónica Avanzada, autorizada para emitir Certificados Digitales, el cual en términos del Código de Comercio es la persona o institución pública que presta servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.
Posteriormente y como consecuencia de ello, va a obtener una Firma Electrónica Avanzada, la cual se define como Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97 del Código de Comercio, que establece:
Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.

[18]"Lo bueno, lo malo y la fea… (tercera y última)" por Carlos Porcel Sastrías. Nota tomada el día jueves 06 de enero de 2011. de la dirección Web: http://www.t21.com.mx/comercio_t21/02.06.07/pdf/pg_7.pdf.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:
I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.
Con lo cual es claro que, como ya lo mencionaba anteriormente, hay un grado de certeza en la relación comercial que permite actuar de manera confiada y segura, logrando reducir tiempos y costos que pueden ser torales en el crecimiento de los negocios".

CONCLUSIONES GENERALES

La iniciativa que presenta el Ejecutivo Federal proponiendo la creación de la Ley de Firma Electrónica Avanzada señala como tal, como *"el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, y que produce los mismos efectos jurídicos que la firma autógrafa"*. Cabe señalar que actualmente ya diversas leyes en México, contemplan este sistema de encriptado de información.

A nivel informático existen diversos con conceptos relacionados con el anterior, que explican la lógica técnica de su funcionamiento.

Dentro de la argumentación que emplea el Ejecutivo en su propuesta señala que "el uso de las tecnologías de la información y comunicaciones en la gestión pública es una opción que debe impulsarse para generar condiciones que permitan hacer más efectiva la provisión de trámites, servicios y procedimientos públicos. Para ello, la iniciativa que se presenta, busca mediante el aprovechamiento de los medios de comunicación electrónica, optimizar y ampliar el acceso y la cobertura a los diferentes trámites y servicios gubernamentales que se proporcionan a la sociedad, así como para lograr una verdadera administración pública "en línea" que permita comunicar a los servidores públicos entre sí y facilitar la interacción entre el gobierno y los ciudadanos, evitando así que éstos realicen desplazamientos innecesarios a los lugares en que se ubican las instituciones públicas, con el consecuente abatimiento de los costos en que incurren los particulares por los traslados y el Gobierno Federal en el uso de papelería".

La Ley de la Firma Electrónica Avanzada está compuesta por los siguientes apartados:

Título Primero Disposiciones Generales
Titulo Segundo de la Firma Electrónica Avanzada
- Del uso y validez de la firma electrónica avanzada
- De los documentos electrónicos y de los mensajes de datos

Título Tercero del Certificado Digital
- De la estructura y procedimientos del certificado digital
- Derechos y obligaciones del titular del certificado digital
- De las Autoridades Certificadoras

- Del reconocimiento de certificados digitales y de la celebración de bases de colaboración y convenios de colaboración o coordinación

Titulo Cuarto de las Responsabilidades y Sanciones

En el ámbito del Derecho Comparado de la estructura (índice) de la legislación existente en materia de Firma Electrónica Avanzada de los países de: Argentina, Chile, España, Perú y Venezuela, pueden advertirse los principales puntos que abordan cada uno de éstos, especificando que los cinco países cuentan con una parte correspondiente referente a “De los certificados digitales” el cual resulta ser un aspecto muy importante ya que permite tener una mayor certeza y seguridad de que no se está haciendo un mal uso de la información y de los datos, entre otros aspectos interesantes en el tema.

Cabe mencionar que sin duda es necesario prestar especial atención al tema correspondiente a los organismos y/o entidades relacionados con la inspección y/o control de la firma electrónica, ya que en sus responsabilidades radica la importancia, seguridad y el adecuado funcionamiento de esta Ley.

Son varios los autores especializados en la materia, que consideran muy relevante los alcances de la regulación de la Firma Electrónica Avanzada, ya que por las circunstancias de globalidad y seguridad que debe haber entre las personas que realizan diversos actos jurídicos a distancia debe de haber certeza y certidumbre en el intercambio de información.

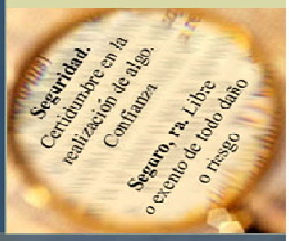
ANEXO

Aplicaciones de la Firma Electrónica[19]

[19] Este documento fue extraído el día jueves 13 de enero de 2011 y puede ser consultado en PDF en la Dirección Web: http://www.seguridata.com/pdfs/presentacion_Firma_electronica.pdf

SeguriData

Aplicaciones de la Firma Electrónica



CONTENIDO

I.- Documento Tradicional

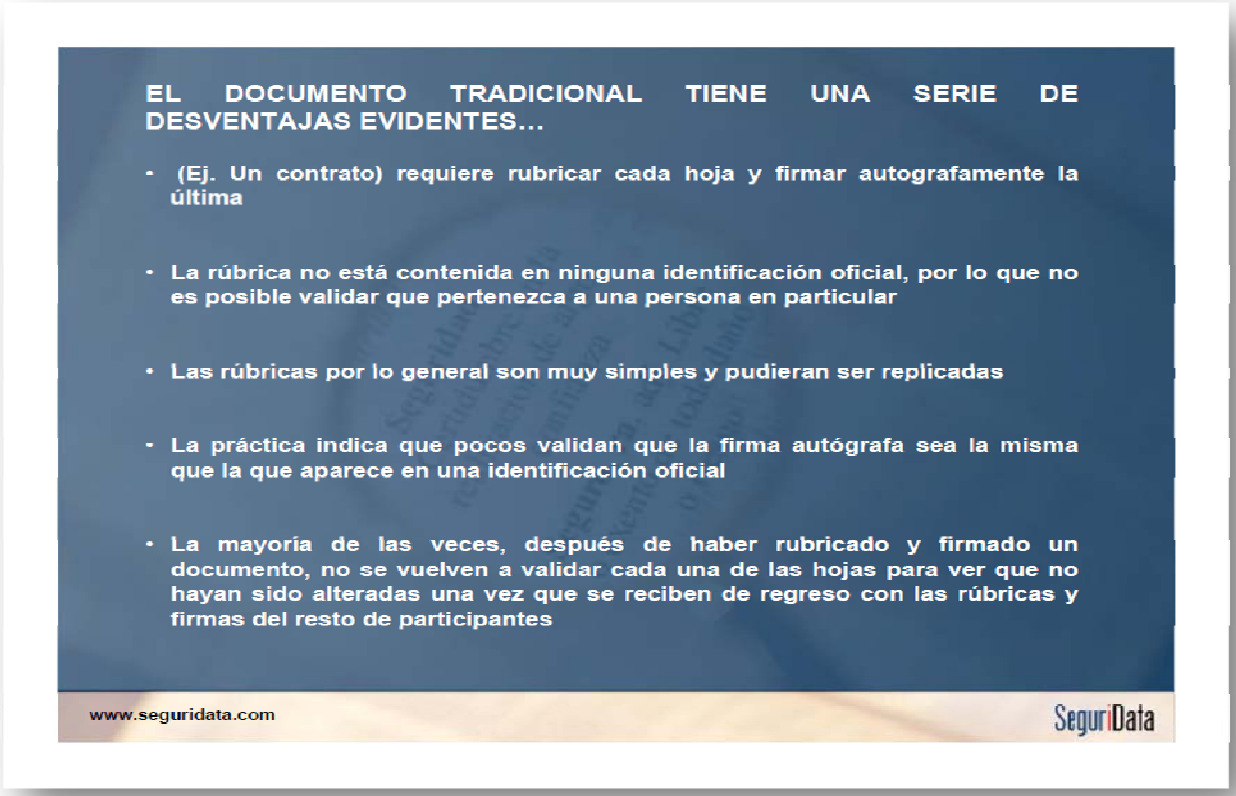
II.- Documento Electrónico Seguro

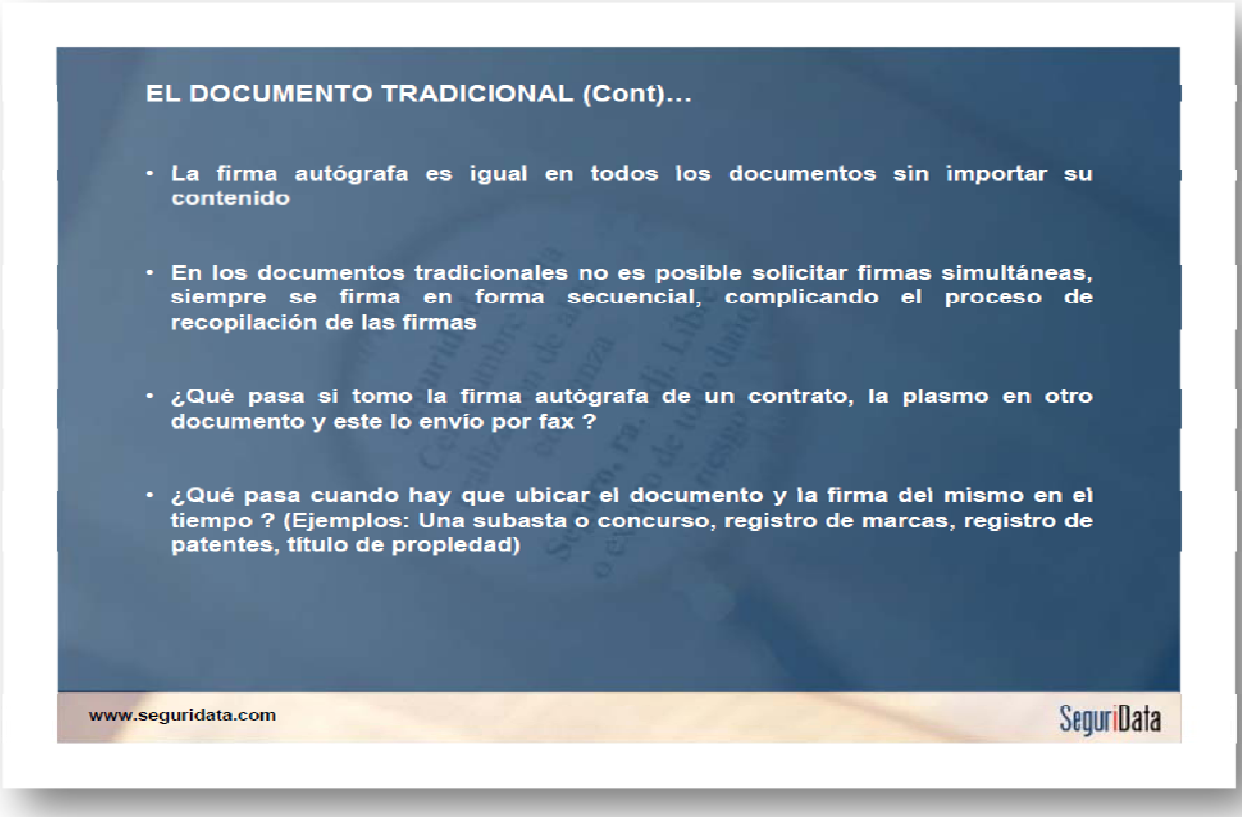
III.- Marco legal

IV.- Conclusión

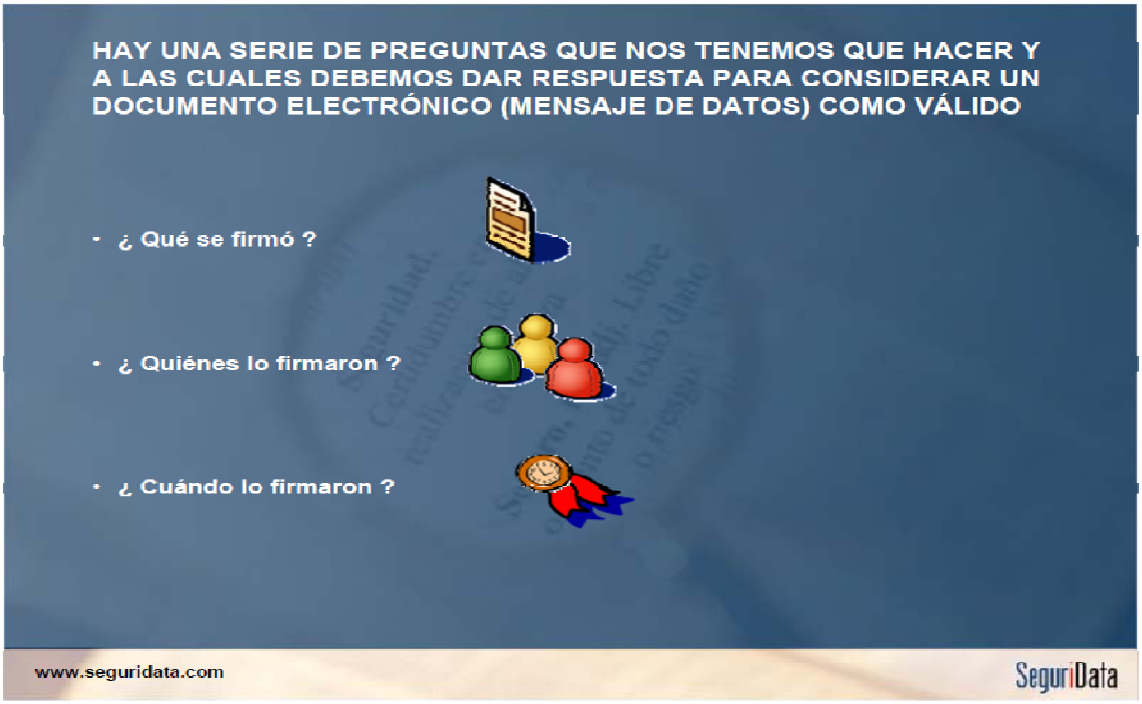
www.seguridata.com SeguriData

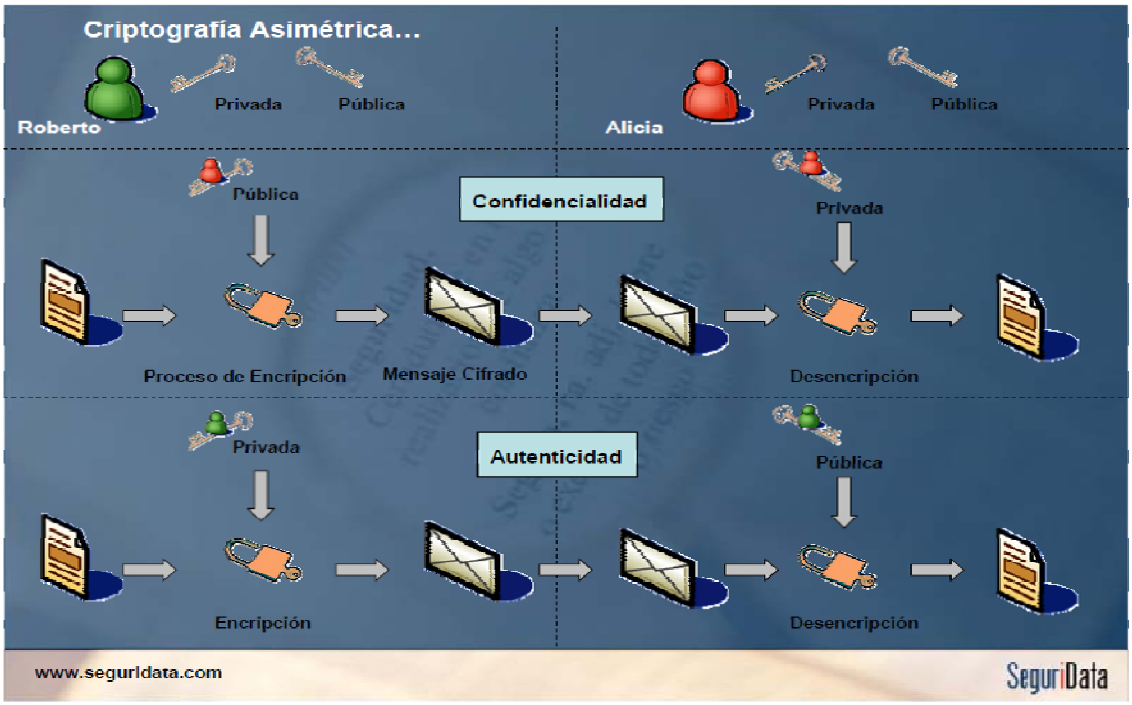

I.- Documento Tradicional
www.seguridata.com
SeguriData

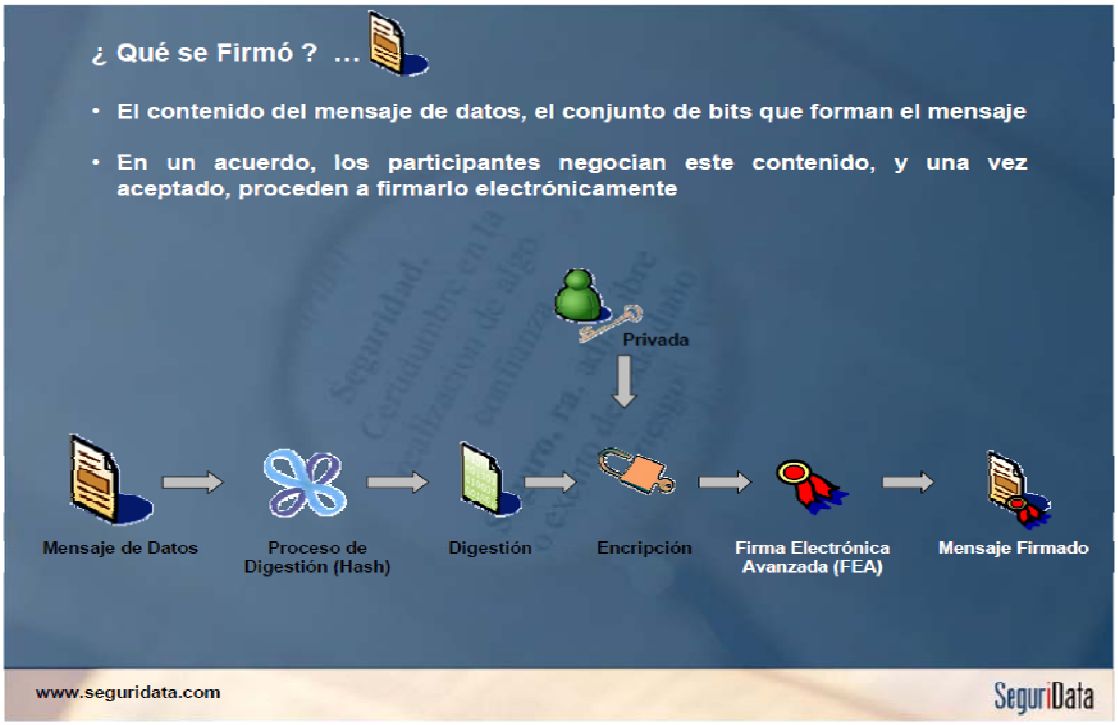

EL DOCUMENTO TRADICIONAL TIENE UNA SERIE DE DESVENTAJAS EVIDENTES...
- (Ej. Un contrato) requiere rubricar cada hoja y firmar autografamente la última
- La rúbrica no está contenida en ninguna identificación oficial, por lo que no es posible validar que pertenezca a una persona en particular
- Las rúbricas por lo general son muy simples y pudieran ser replicadas
- La práctica indica que pocos validan que la firma autógrafa sea la misma que la que aparece en una identificación oficial
- La mayoría de las veces, después de haber rubricado y firmado un documento, no se vuelven a validar cada una de las hojas para ver que no hayan sido alteradas una vez que se reciben de regreso con las rúbricas y firmas del resto de participantes
www.seguridata.com
SeguriData

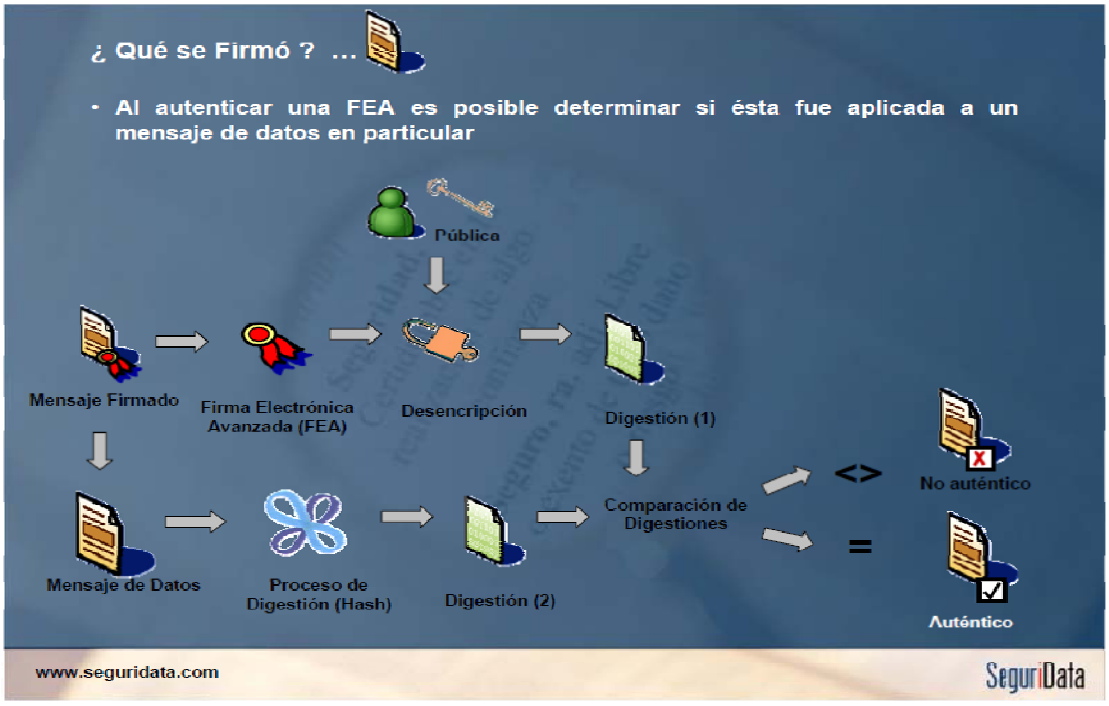

EL DOCUMENTO TRADICIONAL (Cont)...
• La firma autógrafa es igual en todos los documentos sin importar su contenido
• En los documentos tradicionales no es posible solicitar firmas simultáneas, siempre se firma en forma secuencial, complicando el proceso de recopilación de las firmas
• ¿Qué pasa si tomo la firma autógrafa de un contrato, la plasmo en otro documento y este lo envío por fax ?
• ¿Qué pasa cuando hay que ubicar el documento y la firma del mismo en el tiempo ? (Ejemplos: Una subasta o concurso, registro de marcas, registro de patentes, título de propiedad)
www.seguridata.com
SeguriData


II.- Documento Electrónico Seguro
www.seguridata.com
SeguriData

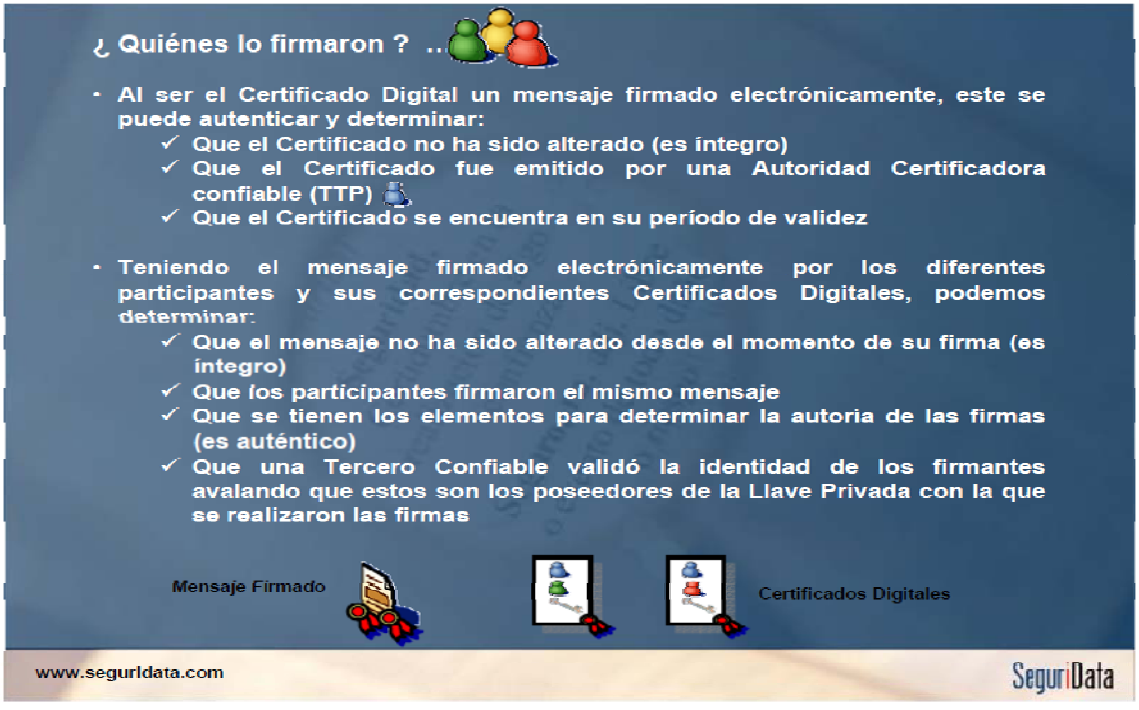

HAY UNA SERIE DE PREGUNTAS QUE NOS TENEMOS QUE HACER Y A LAS CUALES DEBEMOS DAR RESPUESTA PARA CONSIDERAR UN DOCUMENTO ELECTRÓNICO (MENSAJE DE DATOS) COMO VÁLIDO
• ¿ Qué se firmó ?
• ¿ Quiénes lo firmaron ?
• ¿ Cuándo lo firmaron ?
www.seguridata.com
SeguriData


Criptografía Asimétrica...
Roberto
Privada
Pública
Alicia
Privada
Pública
Pública
Confidencialidad
Privada
Proceso de Encripción
Mensaje Cifrado
Desencripción
Privada
Autenticidad
Pública
Encripción
Desencripción
www.seguridata.com
SeguriData


¿ Qué se Firmó ? ...
• El contenido del mensaje de datos, el conjunto de bits que forman el mensaje
• En un acuerdo, los participantes negocian este contenido, y una vez aceptado, proceden a firmarlo electrónicamente
Privada
Mensaje de Datos
Proceso de Digestión (Hash)
Digestión
Encripción
Firma Electrónica Avanzada (FEA)
Mensaje Firmado
www.seguridata.com
SeguriData


¿ Qué se Firmó ? ...
• Al autenticar una FEA es posible determinar si ésta fue aplicada a un mensaje de datos en particular
Pública
Mensaje Firmado
Firma Electrónica Avanzada (FEA)
Desencripción
Digestión (1)
Mensaje de Datos
Proceso de Digestión (Hash)
Digestión (2)
Comparación de Digestiones
<>
=
No auténtico
Auténtico
www.seguridata.com
SeguriData

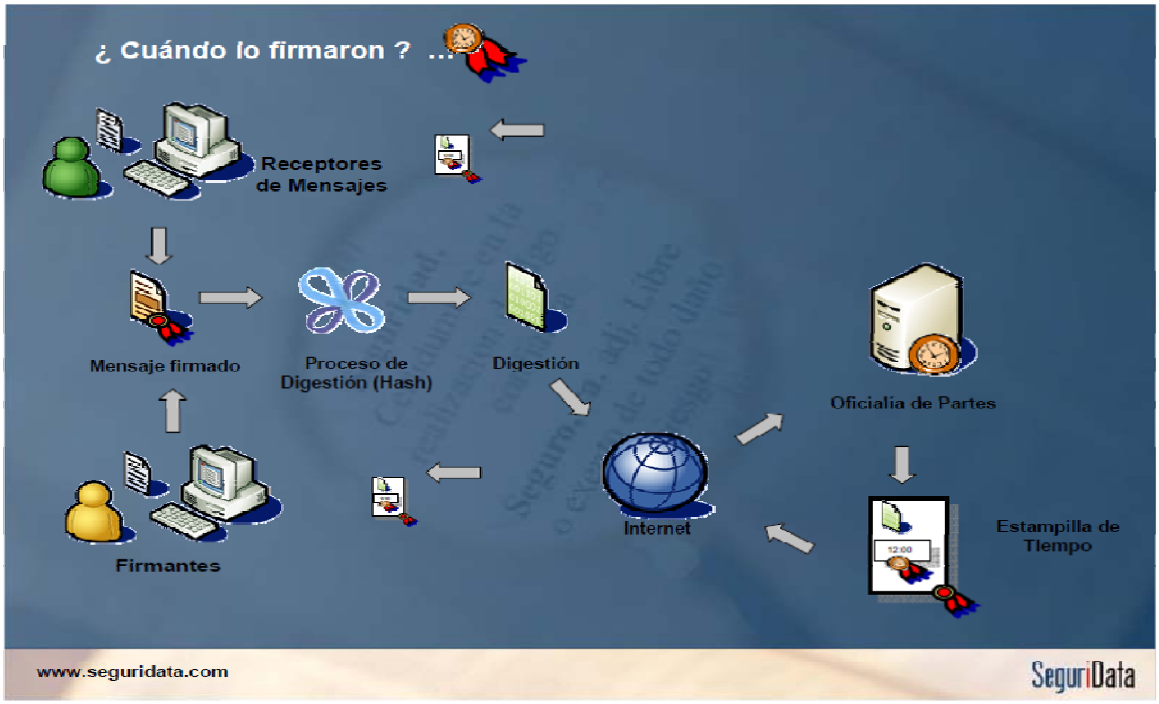

¿ Quiénes lo firmaron ? ...
• Son los participantes que aceptaron el contenido del mensaje de datos y dieron su aceptación utilizando su Llave Privada para generar la FEA
• El Certificado Digital liga la identidad de los firmantes con su Llave Pública, que por su relación con la Privada permite determinar el autor de una FEA
Privada
Pública
Requerimiento de Certificación
Autoridad Certificadora
• Es un tercero confiable (Trusted Third Party - TTP)
• Valida identidad de quien presenta *requerimiento*
• Autentica requerimiento para determinar que el dueño del mismo es propietario de la Llave Privada que corresponde a la Pública dentro del requerimiento
• Agrega sus Datos a los datos del requerimiento, agrega período de validez, asigna número de serie y lo Firma Electrónicamente generando el Certificado Digital
Certificado Digital
www.seguridata.com
SeguriData


¿ Quiénes lo firmaron ? ..
• Al ser el Certificado Digital un mensaje firmado electrónicamente, este se puede autenticar y determinar:
✓ Que el Certificado no ha sido alterado (es íntegro)
✓ Que el Certificado fue emitido por una Autoridad Certificadora confiable (TTP)
✓ Que el Certificado se encuentra en su período de validez
• Teniendo el mensaje firmado electrónicamente por los diferentes participantes y sus correspondientes Certificados Digitales, podemos determinar:
✓ Que el mensaje no ha sido alterado desde el momento de su firma (es íntegro)
✓ Que los participantes firmaron el mismo mensaje
✓ Que se tienen los elementos para determinar la autoría de las firmas (es auténtico)
✓ Que una Tercero Confiable validó la identidad de los firmantes avalando que estos son los poseedores de la Llave Privada con la que se realizaron las firmas
Mensaje Firmado
Certificados Digitales
www.seguridata.com
SeguriData

¿ Cuándo lo firmaron ? ...

- Es necesario determinar si el Certificado Digital del firmante era válido al momento de realizar la firma del mensaje (No Revocado)
  - Si se firmó antes del momento de la revocación, la firma es válida
  - Si se firmó después del momento de la revocación, la firma se considera inválida y se debe rechazar el mensaje
- Es necesario determinar si en su ámbito aplicativo el mensaje tenía validez al momento de su firma (Ejemplo: una subasta o un concurso con fecha límite para entrega de propuestas)
- Es recomendable involucrar a una Autoridad de Estampillas de Tiempo (Time Stamp Authority - TSA) también conocida como Oficialía de Partes, que de fe que una transacción ocurre a cierta fecha y hora a través de la emisión de estampillas de tiempo

www.seguridata.com SeguriData



¿ CUÁLES SON LOS ESTÁNDARES QUE CONTEMPLAN ESTOS CONCEPTOS Y ME PERMITEN DAR RESPUESTA AL QUÉ, QUIÉN Y CUÁNDO ? ...

- X.509 para Certificados Digitales

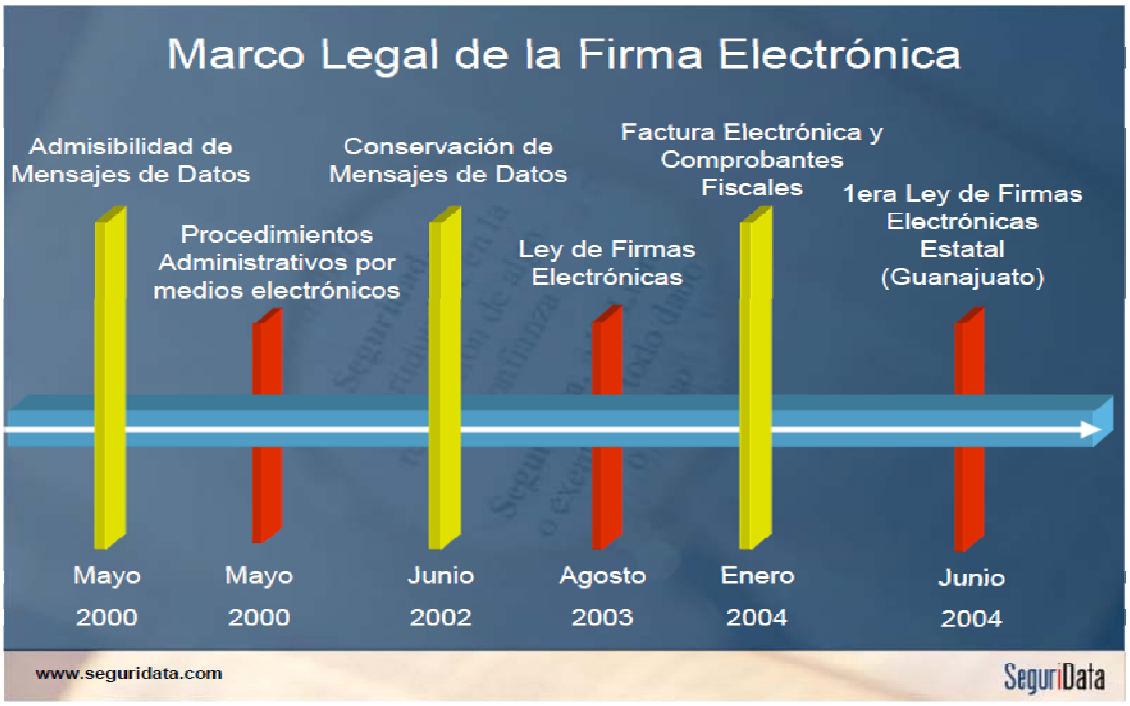
- OCSP (Online Certificate Status Protocol): Permite hacer consultas en línea a las Autoridades Certificadoras sobre el estatus de revocación de un certificado.
- TSP (Time Stamp Protocol): Permite generar estampillas de tiempo que amparan la existencia de un contenido a una determinada fecha y hora.

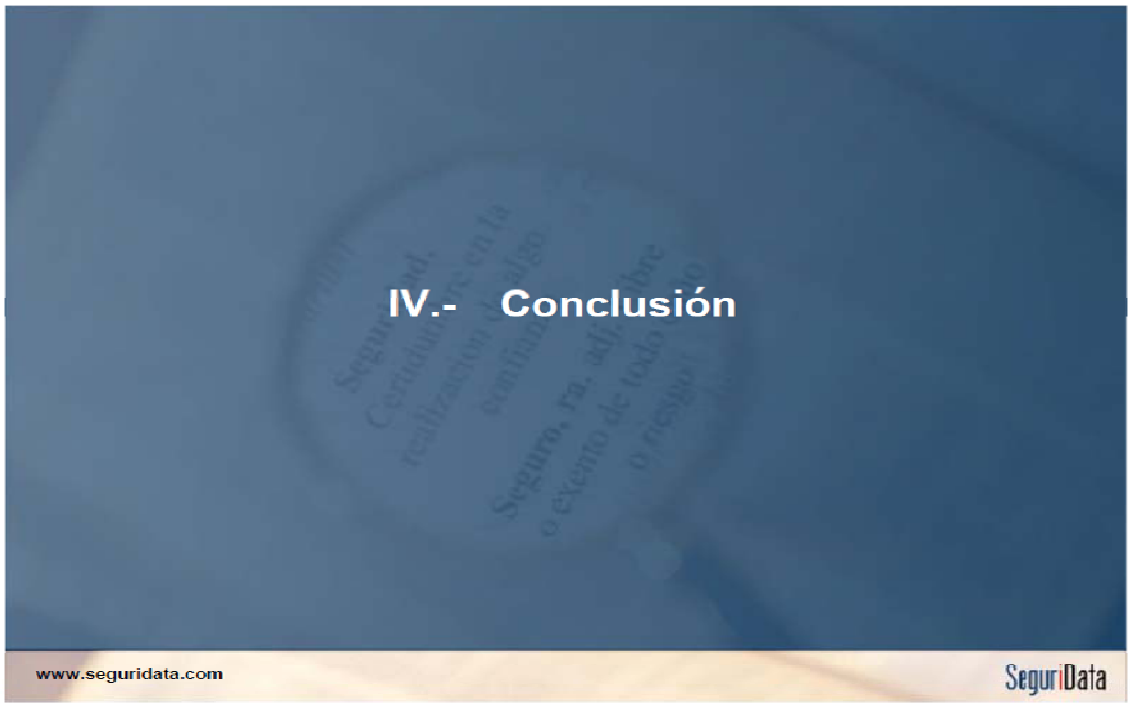
- PKCS (Public Key Cryptography Standards): Estándar que define la Sintaxis de Mensajes Criptográficos, incluyendo mensajes firmados electrónicamente.

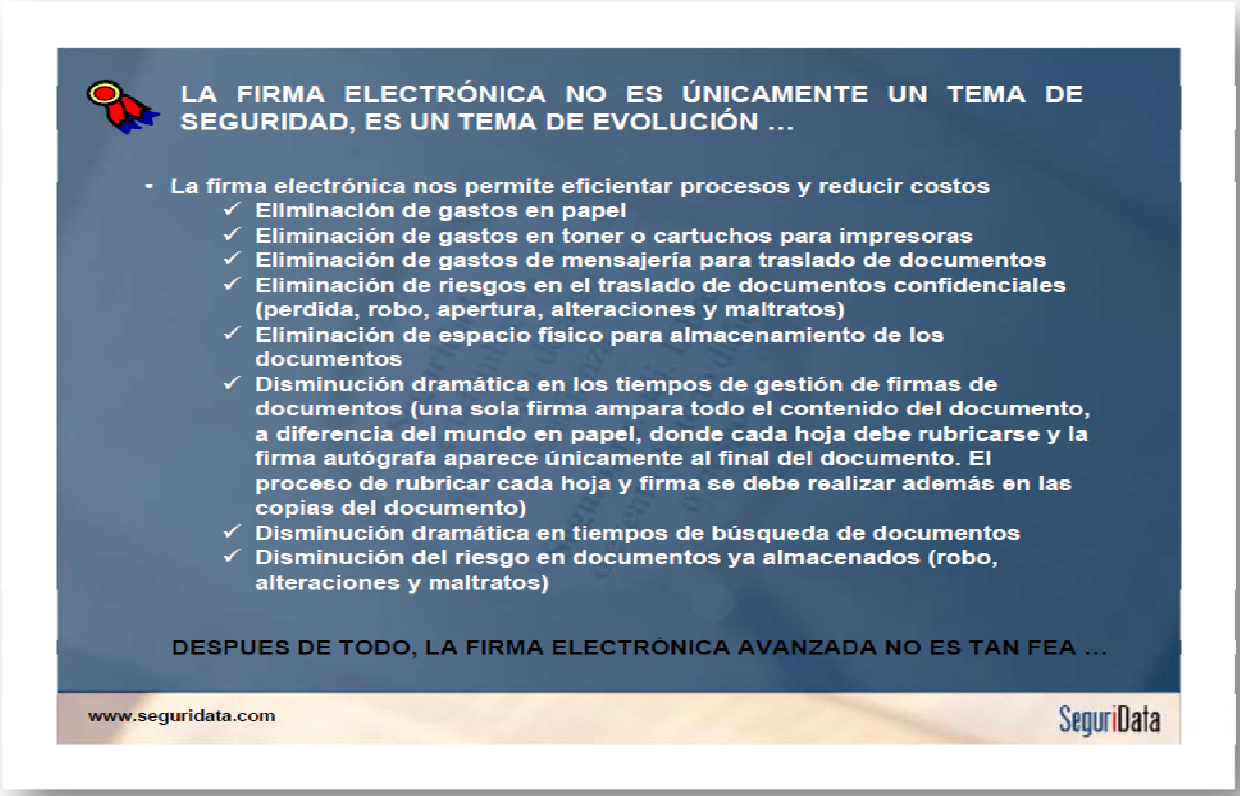
www.seguridata.com SeguriData

III.- Marco Legal

www.seguridata.com SeguriData


Marco Legal de la Firma Electrónica
Admisibilidad de Mensajes de Datos
Procedimientos Administrativos por medios electrónicos
Conservación de Mensajes de Datos
Ley de Firmas Electrónicas
Factura Electrónica y Comprobantes Fiscales
1era Ley de Firmas Electrónicas Estatal (Guanajuato)
Mayo 2000
Mayo 2000
Junio 2002
Agosto 2003
Enero 2004
Junio 2004
www.seguridata.com
SeguriData


IV.- Conclusión
www.seguridata.com
SeguriData


LA FIRMA ELECTRÓNICA NO ES ÚNICAMENTE UN TEMA DE SEGURIDAD, ES UN TEMA DE EVOLUCIÓN …
La firma electrónica nos permite eficientar procesos y reducir costos
Eliminación de gastos en papel
Eliminación de gastos en toner o cartuchos para impresoras
Eliminación de gastos de mensajería para traslado de documentos
Eliminación de riesgos en el traslado de documentos confidenciales (perdida, robo, apertura, alteraciones y maltratos)
Eliminación de espacio físico para almacenamiento de los documentos
Disminución dramática en los tiempos de gestión de firmas de documentos (una sola firma ampara todo el contenido del documento, a diferencia del mundo en papel, donde cada hoja debe rubricarse y la firma autógrafa aparece únicamente al final del documento. El proceso de rubricar cada hoja y firma se debe realizar además en las copias del documento)
Disminución dramática en tiempos de búsqueda de documentos
Disminución del riesgo en documentos ya almacenados (robo, alteraciones y maltratos)
DESPUES DE TODO, LA FIRMA ELECTRÓNICA AVANZADA NO ES TAN FEA …
www.seguridata.com
SeguriData

FUENTES DE INFORMACIÓN

- Iniciativa del Ejecutivo que propone la creación de la Ley de Firma Electrónica Avanzada, presentada ante el Senado de la República el 9 de diciembre del 2010. Dirección en Internet: http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=6754&lg=61

- **ARGENTINA**
  http://www.jgm.gov.ar/paginas.dhtml?pagina=265
  http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
- **CHILE**
  http://repositorio.idiem.cl/ley19799.pdf
- **ESPAÑA**
- entidades de certificación". Editorial Porrúa. México, 2003. Pags. 175 a la 178.
  Real Decreto Ley 14/1999 sobre Firmas Electrónicas
  http://www.csn.es/images/stories/documentos_adjuntos/oficina_virtual/legislacion/RDEC14_1999.pdf
- **PERÚ**
  http://www.policiainformatica.gob.pe/pdf/ley27269.pdf
- **VENEZUELA**
  http://www.gobiernoenlinea.ve/docMgr/sharedfiles/360.pdf
  http://www.tsj.gov.ve/legislacion/dmdfe.htm
- Cámpoli, Gabriel Andrés. "La Firma Electrónica en el Régimen Comercial Mexicano". Editorial Porrúa. México, 2004. Pags. 2 y 3.
- Reyes Krafft, Alfredo Alejandro. "La Firma Electrónica y las
- Presentan Iniciativa de Ley de Firma Electrónica Avanzada; regula su uso en trámites administrativos vía internet; no aplica en casos fiscal, aduanero y financiero". Redacción del periódico la Nota tomada el día miércoles, 05 de enero de 2011 de la Dirección Web:
  http://www.cronica.com.mx/nota.php?id_nota=549176

- Davara, Isabel. "Debate y análisis del uso e impacto de la firma electrónica en México Nuestra "llave" digital". Nota tomada de Blogs de Política Digital, Innovación Gubernamental. Jueves 6 de enero de 2011. Dirección Web:
  http://blogs.politicadigital.com.mx/firma-electronica/?p=328.

- Nota tomada el día jueves 6 de enero de 2011 de la Dirección Web: http://seguridad-de-la-informacion.blogspot.com/2010/07/reflexiones-sobre-certificado-y-firma.html

- Cernuda del Río, Agustín. "Firma Electrónica". Universidad de Oviedo. Artículo tomado el día 06 de enero de 2011 de la Dirección Web:
  http://www.di.uniovi.es/~cernuda/pubs/comercio2002.pdf.

- Ruiz Lancina, María José. **"**La Firma Electrónica: Mayor Seguridad en la Red". Jurista. Licenciada en Derecho y Doctorando en el Departamento de Derecho de la Empresa de la Facultad de Derecho (Universidad de Zaragoza). Nota tomada el día miércoles 05 de enero de 2011 de la dirección Web: http://www.informaticajuridica.com/trabajos/La_firma_electronica_mayor_seguridad_en_la_red.asp.

- Carole Simonnet. "Ley de Firma Electrónica". Viernes, 10 de diciembre de 2010. Nota tomada el día 06 de enero de 2011 de la Dirección Web: http://www.elmanana.com.mx/notas.asp?id=212353

- Lic. Cornejo López, Valentino Francisco. "La Firma Electrónica y su futuro en México". Nota tomada de de la Dirección Web: http://idup.gdl.up.mx/ficheros/firma.pdf.

- Nota tomada el día miércoles, 05 de enero de 2011 de la Dirección Web: http://www.cronica.com.mx/nota.php?id_nota=549176

- "Lo bueno, lo malo y la fea… (tercera y última)" por Carlos Porcel Sastrías. Nota tomada el día jueves 06 de enero de 2011. de la dirección Web: http://www.t21.com.mx/comercio_t21/02.06.07/pdf/pg_7.pdf.

ANEXOS

- Aplicaciones de la Firma Electrónica: Documento extraído el día jueves 13 de enero de 2011 y puede ser consultado en PDF en la Dirección Web: http://www.seguridata.com/pdfs/presentacion_Firma_electronica.pdf

COMISIÓN BICAMARAL DEL SISTEMA DE BIBLIOTECAS

Dip. Aarón Irízar López
Presidente

Dip. Ricardo Sánchez Gálvez
Integrante

Dip. Carlos Torres Piña
Integrante

SECRETARÍA GENERAL

Dr. Guillermo Javier Haro Bélchez
Secretario General

SECRETARÍA DE SERVICIOS PARLAMENTARIOS

Lic. Emilio Suárez Licona
Secretario

CENTRO DE DOCUMENTACIÓN, INFORMACIÓN Y ANÁLISIS

Dr. Francisco Luna Kan
Director General

DIRECCIÓN DE SERVICIOS DE INVESTIGACIÓN Y ANÁLISIS

Dr. Jorge González Chávez
Director

SUBDIRECCIÓN DE POLÍTICA INTERIOR

Mtra. Claudia Gamboa Montejano
Investigadora Parlamentaria
Subdirectora

Lic. Sandra Valdés Robledo
Lic. Arturo Ayala Cordero
Asistentes de Investigación

C. Miriam Gutiérrez Sánchez
Auxiliar de Investigación