Comercio Electrónico, La Firma Digital dentro de las Transacciones Comerciales de lado con el Proyecto de Ley 14.276 "Ley de Firma digital y Certificados Digitales"

Viviana Solís Gómez

2003

INTRODUCCIÓN

La presente investigación tiene una gran importancia y actualidad para el futuro inmediato y óptimo desarrollo del derecho. Con la evolución de la tecnología en los últimos años, sobre todo en el terreno electrónico y digital, ha transformado la operatividad de la industria, del comercio, del sector servicios, de los profesionales, e incluso a nivel doméstico. Los cambios realizados en el ámbito de la información y de la comunicación han contribuido a la modernización de los instrumentos utilizados obteniendo los beneficios de eficacia y rapidez.

Asimismo, en la actualidad son muchos los hogares que se encuentran conectados a Internet por las diversas ventajas que trae su utilización, dado que permite realizar desde operaciones bancarias o financieras hasta encargar la adquisición de todo tipo de productos.

La ley es indispensable para el desarrollo social, cumpliendo la misión de regular los derechos y obligaciones de los ciudadanos de uno o varios países, es por esto que debe cambiar constantemente y

adecuarse a la realidad latente de ese momento, sobre todo cuando la tecnología ha avanzado tanto que prácticamente le exige un cambio.

A estas alturas deberán preguntarse ¿Cuál es el cambio al que nos enfrentamos? Simplemente nos enfrentamos a uno de los más grandes avances de la historia costarricense "La Firma Digital"

"La doctrina jurídica conviene en que la firma es el género, la firma electrónica una especie y dentro de ésta encontramos subespecies, tales como las denominadas en algunas legislaciones como firma digital, firma electrónica avanzada, o firma electrónica certificada".[1]

En esta investigación, el objetivo principal es el estudio de esta figura que hemos denominado "firma digital", en su óptica notarial, civil y comercial, con el fin de demostrar que esta constituye un verdadero elemento tecnológico, legal, válido y eficaz, para la realización de transacciones electrónicas que garanticen seguridad, confidencialidad y agilidad dentro del comercio electrónico, siguiendo con los patrones legales propuestos.

[1] Conclusiones Generales de la Comision de Firma Digital, Dra. Gabriela Guerriero, Dr. Mario Maio, Dra. Marina Mongiardino, Dr. Diego Rull, Dra. Carolina Vega, Dra. Mercedes Velásquez, http://www.aadat.org/conclusiones_generales42.htm

Para llevar a cabo el mejor desarrollo del tema se plantea las siguientes hipótesis:

I.- INTERNET ha propiciado el nacimiento de nuevas figuras, como la firma digital que podrían romper barreras jurídicas, comerciales, territoriales entre otras.

II.- La Firma Digital constituye un elemento tecnológico, legal, válido y eficaz, para la realización de transacciones electrónicas.

III.- Existen insuficiencias en el proyecto de ley 14276, que hacen una necesidad su modificación inmediata, para así evitar futuros tropiezos en nuestra legislación.

Como objetivos generales de la investigación tenemos:

I.- Analizar el proyecto de Ley de Firma Digital y Certificados Digitales Expediente Número Catorce Mil Doscientos Setenta y Seis según parámetros de legislación y doctrina comparada.

II.-Diseñar propuestas al texto sustituyente del Proyecto catorce mil doscientos setenta y seis, que permita una posible aplicación de la Firma Digital.

En cuanto a los objetivos específicos, se han planteado según corresponda con los anteriores los siguientes:

- Determinar la correcta utilización del lenguaje técnico.
- Identificar con otras experiencias comparadas la regulación de deberes y derechos de las entidades certificadoras.
- Hacer un listado de requisitos mínimos que se debe tener para lograr utilizar la firma digital.
- Identificar a las autoridades competentes para la regulación de la Firma Digital.
- Descubrir los vacíos de regulación que existen dentro del proyecto de ley expediente catorce mil doscientos setenta y seis.
- Valorar la legislación y doctrina posiblemente aplicable en Costa Rica.
- Desarrollar a fondo la firma digital para evitar los vacíos de regulación.
- Justificar las propuestas que posiblemente vayan a modificar el proyecto de ley expediente catorce mil doscientos setenta y seis.
- Diseñar un posible texto sustituyente.

El análisis del tema implicará el estudio del origen y evolución de la firma digital de la mano con el derecho, haciendo énfasis en las técnicas y usos de la misma.

Asimismo, se referirá a las transacciones comerciales que se podrían realizar en Costa Rica, de estar aprobada una ley sobre firma digital, sin dejar de lado las ventajas y desventajas que pueda acarrear esta nueva figura, tanto al derecho como a los ciudadanos en general.

Con respecto al proyecto de ley 14276 que existe actualmente en nuestra Asamblea Legislativa denominado "Ley de Firma Digital y Certificados Digitales", se realizará junto a doctrina aplicable y experiencia comparada un análisis del mismo, con el cual se podrá identificar de manera un poco más clara algunas deficiencias que presenta este proyecto.

En la metodología empleada se recurrió al uso de los métodos históricos, sociológicos, inductivos y deductivos; dicha metodología implica tres aspectos: análisis bibliográfico, análisis legislativo y análisis empírico.

La idea fundamental es establecer un cambio entre la normativa y la costumbre existente, contra la realidad imperante y el desarrollo de nuevas tecnologías que dan muestras de la necesidad de una normativa específica.

Actualmente, cada vez son más los bufetes y empresas que deciden adentrarse dentro del mercado virtual, adquiriendo ventajas económicas y eficiencias inalcanzables, al presentarse una verdadera revolución de conocimiento, información y comunicación, que agilizan nuestras economías y presentan grandes beneficios.

Es por esto que nuestro reto como abogados, juristas o administradores de justicia es luchar porque el derecho, la informática y la tecnología se fusionen armoniosamente y lleguen a formar una unión permanente y dinámica que se adecue a la necesidad del hombre como tal.

El presente trabajo de investigación está dividido en tres títulos. Cada título consta de dos capítulos a excepción del último título que solamente posee un capítulo, que a su vez contienen varias sesiones.

El primer título se denomina Generalidades de la Firma Digital y su relación con el derecho, dentro del cual se desarrollaran temas

como antecedentes, nociones generales, origen y evolución de la firma, así como su desarrollo en nuestro territorio.

El segundo título es denominado Técnicas y Usos de la Firma Digital dentro de las Transacciones Comerciales, dentro del cual se desarrollan puntos importantes como técnicas y usos de la firma digital, elementos, requisitos y métodos, ventajas y desventajas, así como sus aplicaciones sobre distintos documentos.

El tercer título es denominado Análisis del proyecto de Ley 14276 "Ley de Firma Digital y Certificados Digitales", junto a doctrina y experiencia comparada, desarrollándose en este último título las consideraciones al proyecto, doctrina aplicable, análisis del articulado y nueva propuesta.

TÍTULO PRIMERO

GENERALIDADES DE LA FIRMA DIGITAL

Y SU RELACIÓN CON EL DERECHO.

CAPÍTULO PRIMERO.

ANTECEDENTES DE LA FIRMA DIGITAL.

SECCIÓN PRIMERA: ORIGEN DE LA FIRMA CONVENCIONAL.

a.- GENERALIDADES DEL COMERCIO ELECTRÓNICO.

El comercio electrónico, por su carácter mundial abarca una amplia gama de actividades, algunas de ellas bien conocidas, la mayoría totalmente nuevas. Impulsado por la revolución de Internet crece aceleradamente y experimenta cambios importantes. Bajo la denominación de comercio electrónico incluyendo tanto el comercio electrónico indirecto (pedido electrónico de bienes tangibles) como el directo (entrega en línea de bienes intangibles). Debido a rápidos cambios, está generando una gran variedad de negocios innovadores, de mercados y de organismos comerciales, con lo cual crea nuevas funciones y nuevas fuentes de ingresos.

Con el advenimiento del comercio electrónico se obliga a replantearse muchas de las cuestiones del comercio tradicional, surgiendo nuevos problemas, e incluso agudizando algunos de los ya existentes. Dentro de los cuales podemos mencionar: la validez legal

de las transacciones y contratos sin soporte de papel, la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio, el control de las transacciones internacionales, incluido el cobro de impuestos; la protección de los derechos de propiedad intelectual, la protección de los consumidores, fraude, estafa, fiabilidad del vendedor y del comprador en una relación electrónica, la falta de seguridad de las transacciones y medios de pago electrónicos, la falta de estándares consolidados, incompatibilidad de legislaciones y la congestión de Internet.

El comercio electrónico "no sólo incluye la compra y venta electrónica de bienes o servicios, que es el concepto común que se tiene, sino que también incorpora el uso de las redes para actividades anteriores o posteriores a la venta, como son: la publicidad, la búsqueda de información, el aseguramiento de las posibles transacciones, el tratamiento de clientes y proveedores, incluso inversores, trámites ante autoridades de control y fiscalización, la negociación de condiciones de compra, suministro, etc., la prestación

de mantenimiento y servicios posventa y la colaboración entre empresas."[2]

El comercio electrónico puede clasificarse en dos: "comercio entre empresas (Businees to Businees) y comercio entre empresas y consumidores (Businees to Consumer). También se habla de comercio electrónico directo e indirecto."[3]

Es por esto que la Secretaría de la UNCTAD (Conferencia de las Naciones Unidas sobre Comercio y Desarrollo), ha preparado un estudio sobre comercio electrónico, titulado "Comercio electrónico: Consideraciones jurídicas", del 20 de mayo de 1998, hace referencia a la revolución tecnológica y el rápido desarrollo del intercambio electrónico de datos (EDI), que el correo electrónico y la Internet están cambiando radicalmente la forma de hacer transacciones comerciales. Haciendo énfasis en el desarrollo de una base legal adecuada que involucre las innovaciones técnicas emergentes.

Entre los primeros intentos de regulación hay que referirse a Ley Modelo sobre Comercio Electrónico aprobada por la CNUDMI

---

[2] De Paladella Salord (Carlos), El Dinero físico y su desaparición?, Argentina, 1999. Documento de Internet disponible: http://www.publicaciones.derecho.org/redi/index.cgi?/N%Famero_10_-Mayo_de 1999/paladella.

[3] Jolene Marie Knorr y Marcelo Roldán Sauma, La Protección del Consumidor en el Comercio Electrónico, 1º edición, Editorial Investigaciones Jurídicas S.A., San José Costa Rica, Julio del 2001

(Comisión de las Naciones Unidas para el Derecho Mercantil Internacional). Esta Ley parte de la observación del número creciente de transacciones comerciales internacionales que se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación habitualmente conocidos como "comercio electrónico", en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan el papel.

En su introducción se considera que la aprobación de la Ley Modelo (se aprobó en junio de 1996) ayudará todos los Estados a fortalecer la legislación o en los casos que carezcan de ella prepararla para el desarrollo de la misma, recomendando a los Estados para que la incorporen a su derecho interno.

El objetivo principal de la Ley Modelo es facilitar el comercio electrónico, ofreciendo un conjunto de reglas internacionalmente aceptables que puedan ser empleadas por los Estados y que de esta forma puedan superar los obstáculos y vacíos jurídicos que existan en relación con el uso de medios de comunicación electrónicos en el comercio tanto nacional como internacional.

Entre los cuales figuran el permitir o facilitar el empleo de formas electrónicas y el de conceder igualdad de trato a los usuarios de documentación consignada sobre papel y a los de información consignada en soporte informático promoviendo la economía y la eficacia del comercio internacional.

En su artículo Primero, indica su ámbito de aplicación, a todo tipo de actividades comerciales que utilicen firmas electrónicas, sin importar si dichas actividades provienen o no de relaciones contractuales, el cual crea un enfoque mucho más abierto.

Es por esto que La Ley Modelo se constituye un texto abierto, donde nada le impide en el futuro incluir nuevas disposiciones para tratar otras materias, reduciendo la incertidumbre con respecto a las consecuencias jurídicas que puedan derivarse del empleo de técnicas modernas, que planten la necesidad de crear una normativa especifica.

Otras iniciativas reguladoras que se han realizado en el ámbito del Derecho Comercial son: "Comité Marítimo Internacional (C.M.I) recopilando conocimientos de embarque electrónicos. El objeto de las reglas C.M.I es establecer un mecanismo para reemplazar el conocimiento de embarque en papel negociable tradicional, por el

electrónico. Son reglas voluntarias y su utilización requiere un acuerdo entre los socios comerciales. El Proyecto Bolero tiene por objetivo crear una plataforma para el intercambio seguro de documentación de comercio electrónico a través de una aplicación de datos central a cargo de la Society for Worldwide Interbank Financial Telecommunications (SWIFT), cooperativa de bancos encargada de la transmisión de mensajes de pago interbancarios y del Through Transport CLUB, (TTtclub), compañía de seguros mutuos que representa a porteadores, agencias de transporte, operadores de terminales y autoridades portuarias. Es otra de las iniciativas dirigidas a reproducir por vía electrónica el conocimiento de embarque negociable tradicional. Tuvo su origen en 1992 e inicialmente recibió alguna financiación de la Unión Europea."[4]

Recordemos que es Estados Unidos el país en el que desde hace años está trabajando de manera intensa en esta materia por lo que ha producido iniciativas como:

El Programa de Comercio Electrónico Federal de los Estados Unidos, que está encargado de coordinar el desarrollo del comercio electrónico dentro del Gobierno Federal de los Estados Unidos,

[4] La Firma y El Comercio Electrónico. Aspectos Jurídicos de Los Servicios de La Sociedad de La Información, Madrid, 7 de diciembre DE 1999. http://www.mju.es/g_firmaelect_amp.htm.

ayudando a las Agencias del Gobierno a encontrar y usar las mejores herramientas de comercio electrónico.

El Commerce Net, que es un consorcio fundado en Sillicon Valley en 1.994, para promover el desarrollo del comercio electrónico a escala global.

La Organización para la Cooperación y el Desarrollo Económico (OCDE), promoviendo la colaboración internacional para minimizar las diferencias entre países en el marco legal del comercio electrónico, incluyendo impuestos, aranceles y derechos de propiedad intelectual.

La Cámara de Comercio Internacional cuyo objetivo es definir buenas prácticas comerciales que ayuden a crear confianza en las transacciones comerciales electrónicas.

La Organización Mundial de Comercio (la OMC) la cual en su conferencia Ministerial de mayo de 1.998, declaró su intención de establecer un amplio programa de trabajo para examinar los aspectos comerciales del comercio electrónico a escala mundial.

La Organización Mundial de la Propiedad Intelectual (WIPO), está mantiene un servidor web sobre comercio electrónico e impulsa los convenios internacionales en esta materia.

b.- NACIMIENTO Y USO DE LA FIRMA CONVENCIONAL.

Para muchos la firma es un fenómeno reciente, pero la realidad es que tiene su nacimiento varias décadas atrás.

No obstante su importancia actual, es relativamente reciente. "En Roma no se firmaban los documentos: ni era costumbre, ni necesario (Cod. Just. VII, 6, 1, 1. Inst. III, 23). La manufirmatio consistía en una ceremonia en que leído el documento por su autor o el notario se lo colocaba desenrollado y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo o una o tres cruces –una por cada persona de la Santísima Trinidad – por el autor o el notario en su nombre, haciéndolo seguidamente los testigos. Más que un requisito la Manufirmatio era en sí misma una parte del espectáculo solemne que se realizaba el acto."[5]

"En la Edad Media se utilizaron sellos, marcas y signos. Estos últimos se formaban con una cruz con la que se entrelazaban en forma arbitraria, letras o rasgos, y fueron usados por los fedatarios hasta hace no mucho. Carlomagno, que apenas sabía escribir hacía

[5] Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 290

firmar sus actos por un sellero oficial, sus sucesores que no mejoraron la cultura del Conquistador utilizaron sellos, hasta que algún tiempo después comenzaron a autenticarse lo documentos con sello y firma, aunque por esto se entendían todavía los signos dibujados para individualizarse. En octubre de 1358, Carlos V. obligó en Francia a los escribanos -que hacia fines del Reinado de San Luis fueron instituidos en oficiales públicos- a suscribir los actos que pasaban ante ellos con sus firmas, además de sus signos. Era en esta época aún tan poco común la escritura que ese mismo año en el Consejo Real eran escasos los que sabían hacerlo, y fue entonces que el mismo Rey dispuso que los actos de ese organismo debían ser autorizados por lo menos por tres de los presentes, los que sí supiesen firmar, estamparían sus marcas o signos."[6]

Con la anterior disposición y el paso del tiempo fue que se dio un mayor desenvolvimiento de las transacciones, la firma como consentimiento entre partes, fue adquiriendo la importancia y las modalidades que ahora tiene consagrada nuestro Código Civil "El Consentimiento de las partes debe ser libre y claramente manifestado.

[6] Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 291

La manifestación puede ser de palabra, por escrito o por hechos de que necesariamente se deduzca."[7], es así como se empieza la cultura del documento escrito o como popularmente se diría "papelitos hablan", donde lo escrito y firmado como ratificación de consentimiento, genera una obligación o como en derecho denominaríamos "Pacta Sunt Servanta"[8].

No podemos dejar de lado la normativa específica correspondiente a la firma como medio eficaz, lo cual se estipula en el artículo 414 del Código de Comercio, "La Firma reproducida por algún medio mecánico no se considera eficaz, salvo los negocios, actos contratos en que la ley o el uso admitan, especialmente cuando se trate de suscribir valores emitidos en número considerable."[9], por ejemplo cuando se confeccionan muchas cartas las cuales deben ir firmadas por el representante lo que la costumbre impone es que se firme una y se fotocopie el resto, debido al tiempo que podría demandar firmar miles y miles de cartas o copias dándole

[7] Código Civil, Artículo1008, 8 Edición, 2001, Editorial Investigaciones Jurídicas.

[8] Guillermo Cabanellas de Torres, Diccionario Jurídico Elemental, Argentina, Editorial Heliasta, 1998, Pág.288, Los pactos han de cumplirse. Esta frase sintetiza la máxima jurídica establecida, con carácter espiritualista, por el Derecho Canónico. "Pacta quantumcunque nuda, Servando sunt" (Aún nudo los pactos hay que cumplirlos).

[9] Código de Comercio, artículo 414, 15 Edición, 1999, Editorial Porvenir

directamente la legitimidad y eficacia a los rasgos realizados por el agente con su puño y letra que la diferencian de las demás firmas.

"Las legislaciones prevén, en general, que la firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada". [10]

Es por esto que se entenderá como firma lo siguiente: "el trazo peculiar mediante el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad."[11]

"Nombre y apellido, o título, que se pone al pie del escrito, para acreditar que procede de quién lo suscribe, para autorizar lo allí manifestado para obligarse a lo declarado."[12]

Planiol y Ripert definen el término estudiado 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."[13]

---

[10] José Alberto Garrone, Diccionario Jurídico, Abeledo-Perrot Tomo II, Buenos Aires, Pág. 156

[11] José Alberto Garrone, Diccionario Jurídico, Abeledo-Perrot Tomo II, Buenos Aires, Pág. 155

[12] Guillermo Cabanellas de Torres, Diccionario Jurídico Elemental, Argentina, Editorial Heliasta, 1998, Pág.169.

[13] Traité practique de Droit Civil Français, VII, núm. 1458, Planiol y Ripert.

Sin embargo entre las distintas definiciones la que considero que se ajusta de una mejor forma a la realidad imperante es la dada por Don José Alberto Garrone que la define de siguiente forma:

"Es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad. Por lo demás no hay exigencia alguna de rúbrica ni obligación de reproducir todas las letras del nombre y apellido. Lo que importa es que la firma configure el modo habitual de signar las manifestaciones de voluntad."[14]

De conformidad con todo lo anterior es que encontramos que a la firma se le pueden dar varios usos, con los cuales es que va a variar el nombre, encontrándose junto a su raíz (firma), el complemento que la describe dependiendo del acto que se realice. Es así como encontramos las siguientes:

Firma a Ruego: es una modalidad sólo aplicable en nuestro Derecho Civil, a los instrumentos públicos, mientras que en el Derecho Mercantil la situación cambia.

"La firma a ruego consiste en la posibilidad que otra persona, distinta en principio, de las partes y de los testigos del acto, suscriba el

[14] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 155

documento a petición o instancias de aquella que no sabe o no puede escribir. El rogado firma, pues, el instrumento público en defecto de la parte que, por un impedimento de tipo permanente –el no saber hacerlo o inhabilidad sobreviviente no recuperable- o de carácter transitorio –imposibilidad de firmar por inhabilidad física recuperable-, no puede firmar por sí misma."[15]

"Carlos E González en su Teoría General del Instrumento Público define la firma a ruego expresando que es "la que hace una persona ajena a su acto o negocio instrumentado, colocando su propia firma a pedido del imposibilitado que es parte interviniente" (edición Ediar, 1953, Pág. 239)"[16]

"El rogado, suscribe el instrumento por el rogante que no puede verificarlo por si mismo, firma a su pedido, sin que por ello importe aseverar o justificar con su acción la certeza o verdad de una cosa, realiza simplemente algo que se le impone y acepta cumplir.

Existe desde tal punto de vista el acuerdo de voluntades exteriorizado por el Derecho Romano con el rogo y el recipio: una persona ruega a otra que ejecute un acto en su nombre y ésta

[15] Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 294

[16]Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 294

contrae esa obligación y la cumple. El firmante a ruego actúa así en representación de uno de los contratantes y hace lo que debía hacer su representado si obrara personalmente, por lo que es parte en el instrumento."[17]

En nuestra legislación dicha figura se encuentra tipificada dentro del artículo 115 del Código Procesal Civil.[18]

Firma Comercial: "nombre que el comerciante usa en ejercicio de su comercio. Bajo ese nombre el comerciante manifiesta como sujeto de derechos y obligaciones en el mundo mercantil: con él contrata, ejecuta los actos relativos a su giro y suscribe los documentos. La función natural de la firma es individualizar al sujeto comerciante. Vivante enseña que por firma se entiende el nombre con que el comerciante ejerce el propio comercio, y tal nombre es normalmente el mismo que corresponde al estado civil del comerciante."[19]

---

[17] Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 295

[18] Código Procesal Civil, Editorial Investigaciones Jurídicas S.A., Gerardo Parajeles Vindas, setiembre de 1999, Pág.52. Artículo 115.- Firma puesta a ruego. Si la parte no sabe firmar o si pese a saber no puede hacerlo por una discapacidad, firmará a su ruego otra persona, en presencia de dos testigos de libre escogencia de la primera. La persona ciega o con deficiencias visuales que lo requiera, firmará por sí misma, en presencia de dos testigos de su libre elección.

[19] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 156

La función fundamental de la firma "…es individualizar, distinguir al comerciante, teniendo en este sentido, un cometido idéntico al del hombre civil. La firma es la imagen genuina de un comerciante, su representación directa. Individualiza, siempre, sujetos de derechos, "el ente capaz de adquirir derechos y contraer obligaciones" en el ámbito del comercio."[20]

Este tipo de firma es sumamente importante para individualizar y ejecutar actos en nombre de la persona jurídica existente, de no existir no podría realizarse una representación eficaz y legitimada del negocio o nombre comercial como tal por lo que todo acto realizado a nombre de la persona jurídica establecida no tendría validez.

Firma a favor en títulos cambiarios: "…la letra de cambio puede garantizarse directamente mediante la suscripción de un tercero determinado. Quien toma la calidad –o posición- de librador, aceptante, endosante e, inclusive, primer tomador, constituyéndose una figura encuadrada dentro del favor cambialis."[21]

[20] Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 304

[21] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 156

"Se caracteriza la firma a favor por:

a) Se trata de facilitar un crédito a otro, pero sin voluntad de responder por el pago.
b) Este aspecto se cumple gratuitamente con el objeto de prestar un servicio."[22]

Esta se constituye como una garantía que brinda la persona física o jurídica de responder por el pago de una obligación y en caso de no pago ejecutar la garantía dada, la cual con anterioridad el firmante aceptó.

Firma de Letrado: "Requisito de carácter eminentemente procesal, importa el patrocinio en el procedimiento escrito y se exige en unos casos, y su conveniencia se impone en otros, atendiendo al orden de regular en los juicios y el interés superior de justicia y el derecho."[23]

"Cuando el litigante presenta escritos, es de norma la asistencia profesional por abogado de la matrícula, y en tal supuesto de petición –toda presentación ante la Justicia concreta una petición- "lleva firma de letrado". El cargo por el actuario, acredita esta circunstancia

[22] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 156

[23] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 157

auténticamente, siendo oportuno consignar, a los fines consiguientes, que el patrocinio también hace responsable al letrado firmante por el contexto del escrito; de ahí y en su caso, las posibles sanciones en los supuestos de extralimitación".[24]

La importancia de este tipo de firma como requisito muchas veces indispensable, radica en la necesidad de que se entienda lo escrito debido a que muchas veces se utiliza un vocabulario más técnico, asimismo de esta forma el letrado asume responsabilidad por lo actuado.

Firma en Blanco: esta puede ser puesta después de llenar el documento, o en blanco para que en otro momento se llene de acuerdo un las instrucciones del firmante.

"La firma en blanco es una forma de mandato que se introdujo en Francia hacia fines del siglo XVII, y que pronto se generalizó en la práctica de los negocios."[25]

Este tipo de firma presenta algunas ventajas y a su vez algunos inconvenientes. Dentro de las ventajas tenemos: "…elimina toda dificultad respecto de los poderes del mandatario que queda habilitado para celebrar cualquier clase de acto que se le

[24] Enciclopedia Jurídica OMEBA Tomo XII Fami-Gara, Buenos Aires, DRISKILL S.A., 1980, Pág. 308
[25] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 157

encomiende. Pero tiene también sus desventajas para el mandante por el riesgo de tener que asumir cualquier compromiso que le endilgue el mandatario."[26]

"Las Firmas en blanco deben ser examinadas en su carácter de instrumentos privados y como actos jurídicos.

Como instrumentos privados, los documentos firmados en blanco en nada se diferencian de los demás instrumentos de aquella índole.

La firma puede ser dada en blanco antes de la redacción por escrito. Después de llenado el acto por la parte a la cual se ha confiado, hace fe siendo reconocida la firma. Es el régimen normal de los instrumentos privados."[27]

No obstante, este tipo de firma acarrea grandes responsabilidades debido a que ha aceptado de antemano lo que pueda estipularse el documento. Por lo tanto, la persona puede quedar comprometida a cumplir obligaciones que no eran precisamente parte de su voluntad.

Firma Entera: es la que está compuesta por el nombre y el apellido completo de la persona que suscribe el acto.

[26] Diccionario Jurídico, Abeledo-Perrot Tomo II, José Alberto Garrone, Buenos Aires, Pág. 157

[27] José Alberto Garrone, Diccionario Jurídico, Abeledo-Perrot Tomo II, Buenos Aires, Pág. 158

La idea de este tipo de firma es que efectivamente pueda comprobarse la identidad de la persona. Una de las costumbres más utilizadas en nuestro medio es la solicitud de la firma como rasgo característico y a su vez del nombre completo consignándose ambas en un mismo documento.

c.- HISTORIA DE LAS TRANSACCIONES ELECTRÓNICAS COMERCIALES.

Después de analizar más detalladamente la firma convencional entraremos a definir un poco más la transacción como parte esencial de nuestro tema por desarrollar, es por esto que entenderemos como Transacción: el "Acto jurídico bilateral, por el cual las partes, haciéndose concesiones recíprocas, extinguen obligaciones litigiosas o dudosas. Es, pues, una de las formas de extinción de las obligaciones. Las cláusulas de una transacción son indivisibles." [28]

Para que la transacción quede establecida se requieren tres elementos:

1. **Acuerdo entre partes**: el consentimiento es un elemento indispensable para realizar cualquier transacción, debido

[28] Dr.Guillermo Cabanellas, Diccionario de Ciencias Jurídicas, Políticas y Sociales, Editorial Heliasta S.R.L. Viamonte 1730.-Piso 1, Buenos Aires República de Argentina, Pág. 759

a que cualquier divergencia de voluntades aunque fueran aspectos secundarios, cambiaria la finalidad.

2. **Reciprocidad de las partes**: la transacción se basa en un intercambio ya sea de derechos como de obligaciones, de esta forma si sólo una de las partes recibe, se estaría frente a una renuncia y no una transacción.
3. **"Res dubia":** la transacción es un negocio o acto jurídico de fijación, la cual deberá determinar la situación dentro de la cual se van a desarrollar las partes.

En lo que se refiere al concepto procesal, "transacción se refiere al término medio en un negocio, sobre todo si se discrepa en el precio. Cualquier ajuste o convenio. Negocio u operación de comercio."[29]

"Una transacción es un conjunto de acciones llevadas a cabo por un usuario o un programa de aplicación, que acceden o cambian el contenido de la base de datos. Las transacciones representan eventos del mundo real, como registrar un inmueble para ponerlo en alquiler, concertar una visita con un cliente a un inmueble,

[29] Diccionario de Ciencias Jurídicas, Políticas y Sociales, Dr.Guillermo Cabanellas, Editorial Heliasta S.R.L. Viamonte 1730.-Piso 1, Buenos Aires República de Argentina, Pág. 759.

dar de alta un nuevo empleado o registrar un nuevo cliente. Estas transacciones se deben realizar sobre la base de datos para que ésta siga siendo un fiel reflejo de la realidad."[30]

"Una transacción puede estar compuesta por varias operaciones, como la transferencia de dinero de una cuenta bancaria a otra. Sin embargo, desde el punto de vista del usuario, estas operaciones conforman una sola tarea."[31]

Es así como encontramos la diferencia entre el contrato como tal y las Transacciones debido a que a pesar de la semejanza, debemos recordar que el contrato es una especie particular de convención cuyo carácter propio consiste en ser productor de obligaciones regulando de una forma más estricta y establecida los derechos y obligaciones, va más allá de registrar un inmueble para ponerlo en alquiler o concertar una visita con un cliente. El contrato por su naturaleza es productor de efectos jurídicos, no es un hecho esporádico o momentáneo debido a que con anterioridad a la celebración de este, las partes han manifestado su voluntad y deseo de reglar sus derechos.

[30] Anónimo, Diseño de Transacciones, http://www3.uji.es/~mmarques/f47/apun/node73.html
[31] Anónimo, Diseño de Transacciones, http://www3.uji.es/~mmarques/f47/apun/node73.html

Existen diversas maneras de clasificar los contratos algunas de estas son: unilaterales y bilaterales, a título oneroso y a títulos gratuitos, consensuales o reales, principales o accesorios, conmutativos o aleatorios.

Las transacciones comerciales nacen espontáneamente cuando una región posee lo que otras desean y no pueden producir o cuando su industria ha adquirido una ventaja relativa en la producción de ciertas cosas. Su expansión ha dependido de muchos factores dentro del cual se encuentra el adelanto tecnológico tanto de los medios de transportes y las comunicaciones, como el sistema bancario y financiero, así como de las leyes de los diversos países.

Durante la historia hemos visto como las caravanas transportaban los productos de Oriente, hasta que los fenicios desarrollaron el comercio marítimo en el mar Mediterráneo, realizado de esta forma todo tipo de transacciones entre diversos pueblos. Es así como después de la Revolución Industrial, el comercio mundial ha estado creciendo de la mano con los progresos de la ciencia, la industria y la tecnología.

Con el paso del tiempo el avance tecnológico ha sido muy importante, realizándose toda clase de proyectos, el más

sobresaliente de los últimos años fue el llevado a cabo por el Departamento de Defensa de Estados Unidos, lo que hoy en día conocemos como la red más grande del mundo: la Internet. Actualmente es accesible en cualquier parte del mundo, ofreciéndonos distintos servicios que ahora podemos decir que son "típicos" para nosotros, entre estos servicios podemos mencionar a las conexiones remotas, la transferencia de archivos, el servicio W W W, los foros de información, y por supuesto el comercio electrónico.

Se calcula que en el próximo año se realizarán cerca de 300.000 millones de dólares en transacciones, solamente en Estados Unidos.

Debido a esta revolución, es que diversas compañías, ciudadanos y países en general demandan la creación de nuevas herramientas y tecnologías para poder establecer sus servicios a través de la Internet.

La gente podrá hacer todo lo que hace hoy, comprar y a vender bienes y / o servicios, llevan a cabo sus transacciones bancarias, aprovechar programas de diversión, realizar operaciones bursátiles, estudiar en otros países obteniendo grados académicos, renovará su licencia de conducir, hacer la compras del

supermercado, etc. Desde la comodidad de su casa u oficina sin tener que trasladarse a ningún lugar, claro está que muchas de las transacciones hoy en día se realizan por medio del Internet, pero no con la seguridad y la confidencialidad que muchos de nosotros deseáramos.

Y es gracias al advenimiento del Internet, las nuevas tecnologías y los nuevos mercados emergentes que se dejan abiertas las puertas para realizar toda clase de transacciones y negocios con más facilidad.

SECCIÓN SEGUNDA. NOCIONES GENERALES SOBRE LA FIRMA DIGITAL Y CERTIFICADOS DIGITALES.

a.- CONCEPTO DE FIRMA DIGITAL.

La firma digital o también llamada firma electrónica avanzada, surge con la idea de sustituir la firma convencional, tradicional o manuscrita como muchos la llaman, especialmente en las transacciones no presenciales (entre ausentes).

"La firma es una forma de exteriorización de la voluntad humana. La voluntad puede manifestarse por diferentes formas, por un gesto, palabras, escritura, fax, etc. La manifestación de la voluntad

en relación con un documento electrónico no puede ser la firma manuscrita".[32]

Es por esto que la ley debe reconocer una forma electrónica de consentir "válida y eficaz para suscribir los documentos electrónicos. Esta forma de consentir - que no es un consentimiento electrónico sino una forma más de manifestación no legislada en nuestro país - es la llamada firma Digital".[33]

Entenderemos por Firma Digital lo siguiente:

"Bloque de caracteres que acompaña a un documento (o fichero) acreditando quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema Criptográfico asimétrica), a la que solo tiene acceso, lo que impide que pueda después negar su autoría (no-revocación o no repudio). De esta forma, el autor queda vinculado al documento de

32 Conclusiones Generales de la Comisión de Firma Digital, Dra. Gabriela Guerriero, Dr. Mario Maio, Dra. Marina Mongiardino, Dr. Diego Rull, Dra. Carolina Vega, Dra. Mercedes Velásquez, http://www.aadat.org/conclusiones_generales42.htm

33 Conclusiones Generales de la Comisión de Firma Digital, Dra. Gabriela Guerriero, Dr. Mario Maio, Dra. Marina Mongiardino, Dr. Diego Rull, Dra. Carolina Vega, Dra. Mercedes Velásquez, http://www.aadat.org/conclusiones_generales42.htm

la firma. Por último, la validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor."[34]

Es considerada a su vez "un conjunto de datos que se añaden al contenido de una transmisión y permiten que el receptor pueda comprobar la integridad de la información enviada y la veracidad d la fuente"[35]

Según MSc. Christian Hess Araya, en los "Comentarios al Proyecto de Ley de Firma Digital de Costa Rica"[36], de fecha 19 de febrero del 2001, afirma que la firma digital, en síntesis, es el resultado de encriptar (codificar), empleando una clave privada, un conjunto de datos que -a su vez- son el resultado de aplicar a un documento o mensaje lo que denominamos una "función hash" (procedimiento capaz de generar una representación simbólica, matemática, del original). El documento o mensaje, con su correspondiente firma digital, es enviado al destinatario, quien -empleando la correlativa clave pública del remitente- puede desencriptar la firma digital y

[34] Como Aplicar la nueva normativa sobre la firma electrónica, Fernando Ramos Suárez, Febrero 2000, Documento disponible en Internet: http://www.legalia.com

[35] Revista de Ciencias Jurídicas, Universidad de Costa Rica, Dr. Jorge Enrique Romero Pérez, Nº 97-cuatrimestral, enero-abril-2002, Pág. 121

[36] Si se desea conocer más acerca de estos comentarios al proyecto de ley se puede acudir a la página http://comunidad.derecho.org/chess/publicac/firmadigital.html

confrontar el resultado con el texto original. Una comparación exacta prueba irrefutablemente (para todos los efectos prácticos, al menos) que el mensaje proviene del tenedor de la clave privada y que no ha sido alterado en tránsito.

La firma digital constituye un elemento válido, tecnológico, legal y eficaz que posibilita la realización de transacciones electrónicas comerciales seguras a través de redes de información. "Su implementación permitirá firmar contratos a través de la red, adquirir bienes y servicios, realizar pagos, votar o cualquier otra actividad donde se requiera identificación de autoría."[37]

Hoy en día, se han implementado diversas normas sobre firmas digitales y electrónicas con fines privados y públicos, que autorizan la existencia de autoridades certificadoras las cuales funcionan como una especie de notario cibernético, autenticando en línea de manera inmediata la firma digital del usuario.

En Estados Unidos, Europa, Alemania e Italia se cuenta con leyes en esta materia, que regulan la firma digital y electrónica y sus derivaciones. Procurando no especificar el tipo de comercio por

[37] La Protección del Consumidor en el Comercio Electrónico, Jolene Marie Knorr y Marcelo Roldán Sauma, 1º edición, Editorial Investigaciones Jurídicas S.A., San José Costa Rica, Julio del 2001, Pág. 73

desarrollar con esta figura, dejando abierta la posibilidad de desarrollar diversos tipos de transacciones con ella.

La ley del Estado de Utah sobre la Firma Digital, de Estados Unidos de Norteamérica (1996) define la firma digital ("dig-sig") como la trasformación de un mensaje empleando un criptosistema asimétrico tal que una persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza: i. Si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y ii. Si el mensaje ha sido modificado desde que se efectúo la transformación.

La firma digital utiliza un criptosistema asimétrico. "Esto significa que comprende dos procesos: i. la creación de la firma por el suscriptor utilizando la clave privada, que es sólo conocida por el suscriptor, y es el único responsable de su guarda, ii. la verificación de la firma por la otra parte: el receptor del mensaje comprueba su autenticidad utilizando la clave pública que surge del certificado del suscriptor, comunicándose con el repositorio o registro donde el referido certificado se encuentra registrado."[38]

[38] Banca, Comercio, Moneda Electrónica y La Firma Electrónica, Mauricio Devoto y Horacio M Lynch, www.v2.vlex.com.es

En Costa Rica, nuestra legislación parece ser que deja por fuera el valor jurídico de la firma digital, estableciendo en el Código de Comercio, artículo 414 lo siguiente:

"La Firma reproducida por algún medio mecánico no se considera eficaz, salvo los negocios, actos contratos en que la ley o el uso admitan, especialmente cuando se trate de suscribir valores emitidos en número considerable. Este es uno de los grandes problemas que presentara la firma al desarrollarse la firma."[39]

En referencia a lo mismo la Procuraduría General de la República de Costa Rica señala:

"…dado que la Firma Digital funciona dentro de los círculos de correspondencia de signatarios que emiten y aceptan como firmas las combinaciones de caracteres que las sustituyen y que aceptan como firmas las combinaciones de caracteres que las constituyen y que aceptan la constatación de una autoridad certificadora superior, su reconocimiento como valor jurídico en nuestro medio no es posible, dado que la regulación misma como el establecimiento de las

39 Art.414 del Código de Comercio, 15 Edición, 1999, Editorial Porvenir

autoridades certificadoras correspondientes deben ser creadas por ley."[40]

No obstante, de lo anterior dejando el criterio establecido por La Procuraduría y basándonos en el Código de Comercio podríamos interpretar que en "Costa Rica la firma electrónica (reproducida por medios mecánicos) sí debería ser permitida al menos en los casos en que los usos o costumbres comerciales así lo admitan y requieran."[41] como lo es el derecho privado.

b.- DIFERENCIAS ENTRE FIRMA ELECTRÓNICA Y FIRMA DIGITAL.

Es común que estos dos términos se confundan constantemente, a pesar de la gran diferencia que existe a la hora de utilizarlas y los efectos que ambas producen. Es por esto que considero importante identificarlas y definirlas para así evitar confusiones en el desarrollo de la presente investigación y en general para la vida cotidiana.

La firma electrónica se entiende como "aquel conjunto de datos en forma electrónica, ajenos a otros datos electrónicos o

[40] Procuraduría General de la República, Dictamen C-283-98, dirigido al Archivo Nacional el 24 de diciembre de 1998.

[41] Jolene Marie Knorr y Marcelo Roldán Sauma, La Protección del Consumidor en el Comercio Electrónico, 1º edición, Editorial Investigaciones Jurídicas S.A., San José Costa Rica, Julio del 2001, Pág. 75

asociados funcionalmente a ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge."[42]

Asimismo, la Licda. Teresa Pérez Porta, en su Informe Técnico, del Proyecto "Ley de Firma Digital y Certificados Digitales", Expediente Nº 14276, elaborado para la Asamblea Legislativa define: que la firma electrónica es cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte, con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

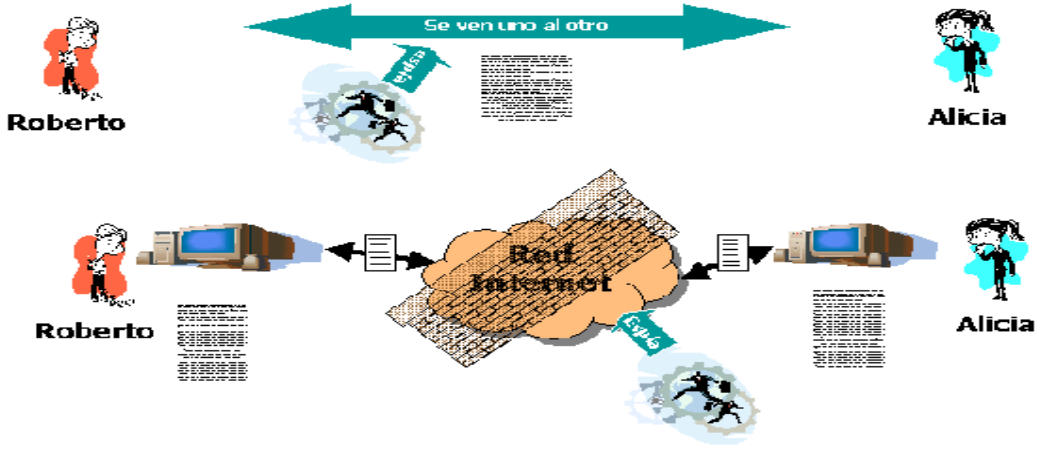
Por consiguiente, podríamos decir que es la firma que se realiza mediante medios electrónicos, con el fin de crear un vínculo de reconocimiento sobre el documento signado, para que de esta forma el receptor del documento pueda identificar de una manera formal a su autor.

Ejemplo de esto sería la simple firma de cualquier documento por algún medio mecánico, reconociendo únicamente que ese documento posiblemente pertenece a quien dice ser, y se dice

[42] Fernando Ramos Suárez, LEGALIA "Compañía de Servicios Jurídicos", www.legalia.com

"posiblemente" porque no tiene la seguridad, integridad y confidencialidad.

Diferencia entre firma manuscrita y firma electrónica.[43]



En el anterior dibujo se muestra la diferencia entre la firma manuscrita y la firma electrónica, no obstante ambas firmas están expuestas a los espías.

Mientras que la firma digital es un proceso de encriptación que traduce el documento por medio de un algoritmo Hash y una clave privada, para que este sea incomprensible tanto para terceros que puedan interceptar el documento, como para el receptor que no aplique la clave pública determinada.

[43] Guía Telemática, http://www.diputados.gov.ar/guia_tematica.html

Asimismo, "permite la identificación del signatario y ha sido creada por medios que este mantiene bajo su exclusiva 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 estos."

Esto debido a que está basada en el uso de un par de claves asociadas, una clave privada que se debe mantener en secreto, tal y como un pin de la tarjeta de crédito, y una clave pública, libremente accesible por cualquier persona.

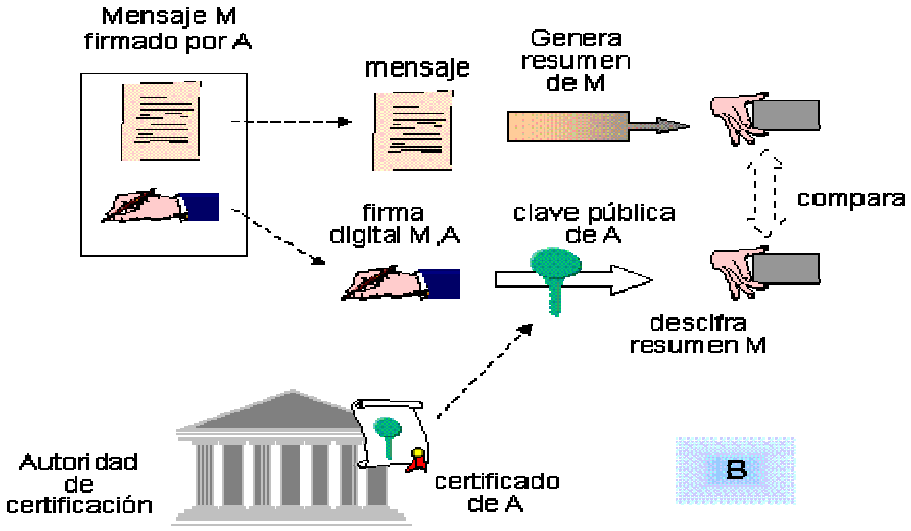
La trasformación del mensaje al cual se le aplica la firma digital deberá realizarse de la siguiente forma:

1. Si un mensaje fue firmado con la clave privada del firmante, sólo puede ser verificado por el receptor utilizando la clave pública de ese mismo sujeto.
2. Si el mensaje fue firmado con la clave pública del receptor, sólo puede ser verificado por el receptor utilizando su propia clave privada.

Por lo que si el mensaje inicial ha sido alterado después de enviado por el firmante, sin importar si la alteración fue mínima, el documento firmado no coincidirá y se mostrará de una manera

ilegible para el receptor, garantizando de esta forma la integridad, autenticidad y confidencialidad del mismo.

Firma Digital[44]



c.- CARACTERÍSTICAS DE LA FIRMA DIGITAL.

Al hablar de firma digital debemos hacer énfasis en ciertos principios que deben regular el marco normativo algunos de estos son: la libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia de la firma digital a la firma manuscrita, el respeto a las normas documentales existentes, el reconocimiento de los efectos jurídicos, la no discriminación del documento firmado

[44]Estudio de la situación del comercio electrónico en España, http://www.internautas.org/documentos/

digitalmente, la libertad contractual, la limitación de responsabilidad y sus sanciones.

1. **Establecer la libre competencia**. No crear limitaciones en relación con todos los servicios de certificación, al sujeto que la utiliza ni mucho menos a la firma electrónica utilizado, dejando posibilidad al libre mercado.
2. **Asegurar la neutralidad tecnológica**. No discriminación entre distintas tecnologías y, en consecuencia la necesidad de producir normas que regulen los diversos entornos tecnológicos. Dejando la flexibilidad que deben tener las normas, al no estar condicionadas a un formato, una tecnología, un lenguaje o un medio de transmisión específico.
3. **Promover la compatibilidad con el marco jurídico internacional.** Este principio se refiere a nivel internacional, procurando incorporar una normativa común o por lo menos semejante entre distintos países y estados al aplicar la firma digital.
4. **Establecer la equivalencia de la firma digital a la firma manuscrita**. Deberá considerarse el requisito de firma, satisfecho respecto de los datos consignados en forma electrónica,

atribuyéndole los mismos efectos jurídicos que la firma manuscrita con relación a los datos consignados en papel.

5. **Respeto a las normas documentales existentes**. La utilización de nuevas técnicas y en especial de la firma digital no debe ir en disminución de la firma manuscrita, debido a que la utilización de ambas debe ser siempre de manera voluntaria, asimismo no se debe alterar los diversos actos jurídicos y notariales, sino procurar que la utilización de la firma digital no carezca de efectos jurídicos debido a su naturaleza digital.
6. **Reconocimiento de los efectos jurídicos de las firmas digitales**. Asegurar el reconocimiento de los efectos jurídicos de las firmas digitales, así como de su procedimiento y mecanismos tanto a nivel nacional como internacional.
7. **No discriminación del documento digital firmado digitalmente**. Se deberá crear dentro de la legislación una norma que garantice la fuerza probatoria y ejecutoria de la firma digital. Asegurar que esta tendrá efectos jurídicos y no será desvirtuada ni cuestionada por el sólo hecho de presentarse en un formato digital, reconociéndolas de igual manera que una firma convencional.

8. **Libertad Contractual**. Deberá permitir a las partes convenir entre ellas la forma en que realicen sus transacciones, el territorio, el tiempo, el modo, la forma de pago y demás que determinen las partes; pudiendo ellas de igual forma elegir si realizan su transacción utilizando la firma digital o convencional según lo acordado.
9. **Limitación de responsabilidad**. Limitación de la responsabilidad haciendo constar en los certificados que se emitan y en los acuerdos que aceptan las partes, las restricciones establecidas para su utilización, modificación y aceptación de lo pactado.
10. **Sanciones**. Al otorgarle efectos jurídicos al documento firmado digitalmente, este en consecuencia deberá de penalizar ciertas acciones como estafas o falsificaciones que se puedan realizar utilizando la firma digital o cualquier otra tecnología similar.

Existen dos propósitos centrales al firmar digitalmente un documento electrónico:

1.-"Garantizar su **autenticidad**, informando de manera cierta acerca de su autoría (no sólo en cuanto a la identidad del autor sino eventualmente incluso en cuanto a la hora y

fecha precisas de su redacción) y, por esta vía, contribuyendo a evitar una posible repudiación de sus consecuencias legales o de otra índole…"[45]

Estamos de esta manera comprobando que la persona que envía el documento es quien dice ser realmente.

2.-"Garantizar su integridad, en la medida en que permite asegurar que el contenido del documento no ha cambiado desde su firma."[46]

La firma digital detecta la integridad de la información que fue firmada, asegurando que esta no haya sido modificada; de ser modificada esta durante el proceso de envío, el mensaje de datos, al agregarle la clave respectiva no será legible.

Con la firma digital se pretende cumplir con las mismas tres funciones que caracterizan a la firma convencional, manuscrita u ológrafa como muchos la denominan de las cuales se hace una breve mención.

[45] "La firma digital para abogados y notarios", MSc. Christian Hess Araya, El Foro, Revista del Colegio de Abogados de Costa Rica, Año I/ Número 2, Setiembre 2002, Pág. 43 y 44.

[46] "La firma digital para abogados y notarios", MSc. Christian Hess Araya, El Foro, Revista del Colegio de Abogados de Costa Rica, Año I/ Número 2, Setiembre 2002, Pág. 43 y 44.

1. **Función indicativa:** "…revela la identidad del autor de un documento."[47], podemos precisar quien es el autor del documento, el momento en que se envío entre otros aspectos.
2. **Función declarativa:** "por medio de la cual se entiende que una firma implica la aceptación del autor del contenido del documento…"[48], creando una responsabilidad hacia el autor del mismo.
3. **Función probatoria:** "permite vincular jurídicamente a un documento con su autor, para efectos demostrativos."[49]

Los elementos que clasifican e identifican a la firma digital de otras figuras, haciendo de esta un medio más seguro, rápido y eficaz son los siguientes:

1. **Confidencialidad:** "requiere que la información sea accesible únicamente por las entidades autorizadas. La

[47] "La firma digital para abogados y notarios", MSc. Christian Hess Araya, El Foro, Revista del Colegio de Abogados de Costa Rica, Año I/ Número 2, Setiembre 2002, Pág. 43 y 44.

[48] "La firma digital para abogados y notarios", MSc. Christian Hess Araya, El Foro, Revista del Colegio de Abogados de Costa Rica, Año I/ Número 2, Setiembre 2002, Pág. 43 y 44.

[49] "La firma digital para abogados y notarios", MSc. Christian Hess Araya, El Foro, Revista del Colegio de Abogados de Costa Rica, Año I/ Número 2, Setiembre 2002, Pág. 43 y 44.

confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos…"[50], mediante algún tipo de cifrado.

2. **Autenticación:** "requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa." [51]Se distinguen dos tipos:

   2.1 **De entidad. "**Asegura la identidad de las entidades participantes en la comunicación, mediante características biométricas (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares."[52]

   2.2 **De origen de información.** "Asegura que una unidad de información proviene de cierta entidad,

[50] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 87

[51] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 89.

[52] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 89.

siendo la firma digital el mecanismo más extendido."[53]

3. Integridad. "requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye la escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera …"[54], y como habíamos dicho antes logra asegurar el contenido.

4. No repudio. "Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación…"[55], de esta forma al aplicar la figura de la firma digital está aceptando su responsabilidad y comprometiéndose con el documento firmado que corresponde a su autoría, por lo que no se puede negar.

---

[53] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 89.

[54] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 89.

[55] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 89.

5. Control de acceso. "requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema de destino, mediante el uso de contraseñas o llaves hardware, protegiéndolos frente a usos no autorizados o manipulación."[56], para que el mensaje sea enviado eficientemente debe ingresar el código o clave privada a la que sólo el usuario tiene acceso, asimismo debe existir un registro donde los usuarios puedan acceder fácilmente y comprobar que la clave pública y el certificado están vigentes.

6. Disponibilidad. Los recursos tanto para verificar como para utilizar la firma deben de estar disponibles al usuario y a las entidades autorizadas cuando lo necesiten.

d.- CONCEPTO Y CARACTERÍSTICAS DE LOS CERTIFICADOS DIGITALES.

Los Certificados son "registros electrónicos que atestiguan que una clave pública pertenece a un determinado individuo o entidad.

[56] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 90

Permite la verificación de que una clave pública dada pertenece fehacientemente a una determinada persona."[57]

El MSc. Christian Hess, en sus Comentarios al Proyecto de Ley de Firma Digital (Pág. 4, 2001), indica que un certificado digital deberá contener el nombre del usuario, su clave pública, un número de serie y una fecha de expiración.

De igual forma Mauricio Devoto y Horacio M. Lynch, hacen referencia a que el certificado en su forma más simple, contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado.

Estos certificados se inscriben en un Registro o como en ocasiones lo denominan repositorio (repository), "considerado como una base de datos a la que el público puede acceder directamente en línea (on-line) para conocer acerca de la validez de los mismos."[58]

Los usuarios o firmantes son: "…aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en

[57] Mauricio Devoto y Horacio M, Banca, Comercio, Moneda Electrónica y La Firma Electrónica, Lynch, www.v2.vlex.com.es

[58] Mauricio Devoto y Horacio M, Banca, Comercio, Moneda Electrónica y La Firma Electrónica, Lynch, www.v2.vlex.com.es

el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante de tal forma que quién pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante."[59]

Existen diversos tipos de certificados que la autoridad certificante[60] puede emitir:

1. **Certificados de identificación:** los cuales deberán identificar y conectar un nombre a una clave pública.
2. **Certificados de autorización:** estos indican oto tipo de información al usuario, tales como dirección, antecedentes, productos, etc.
3. **Certificados en el papel de notario:** los cuales serán utilizados para dar fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.

[59] Fernando Ramos Suárez, "Como Aplicar La Nueva Normativa Sobre La Firma Electrónica", Op. Cit.

[60] Según el proyecto de Ley que se encuentra en la Unidad de Asuntos Jurídicos en La Asamblea Legislativa número 14276, artículo 11.- La Autoridad Certificante o Autoridad Acreditadora como se nombra en el proyecto será un órgano subordinado al Ministerio de Ciencia y Tecnología.

4. **Certificados de determinación:** permiten determinar el día y hora en que el documento fue firmado digitalmente. (Digital time-stamp certificates).[61]

"La certificación en redes abiertas utiliza certificados basados en el estándar (X.509 v3) que permite:

1. Firmar digitalmente los mensajes de tal forma que el receptor pueda descifrarlos y tener acceso a su contenido, garantizando la autenticidad y el no repudio.

2. Cifrar la información (encriptación) de tal forma que sólo el receptor pueda descifrarlos y tener acceso a su contenido, garantizando su integridad y confidencialidad.

3. Proporcionar seguridad y autentificar la identidad de acceso de los usuarios de Intranets/Extranets."[62]

A nivel mundial la mayor Autoridad de Certificación es Verising cuyos certificados vienen incluidos "de fabrica" en los navegadores como Netscape o Explorer.

Existen otros sistemas que utilizan el cifrado y la firma digital, como PGP, que no utilizan autoridades de certificación externas, sino

[61] Si desea ampliar más el tema concerniente a certificados digitales, su utilización y ejemplos puede acudir a la pagina electrónica www.lagalia.com, así mismo si desea evacuar consultas puede dirigirse al correo electrónico framos@lagalia.com con el Lic. Fernando Ramos Suárez.
[62] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Op.Cit. Pág. 101.

que delegan en el propio usuario la responsabilidad de aceptar claves conforme a su criterio, estableciendo una red de confianza (Web of Trust) totalmente descentralizada, pero con el apoyo de una red de servidores de claves. Este sistema se basa en la buena fe de todos los usuarios participantes y no proporciona autenticación de las partes en forma estricta.

CAPÍTULO SEGUNDO.

ORIGEN Y EVOLUCIÓN DE LA FIRMA DIGITAL.

SECCIÓN PRIMERA: DESARROLLO DE LA FIRMA DIGITAL EN EL MUNDO.

a.- INICIATIVAS EUROPEAS

La primera aproximación al fenómeno del comercio electrónico, fue en 1989, como parte de su programa TEDIS (Trade Electronic Data Interchange System) o lo que en español significaría Sistema de Intercambio Comercial de Datos.

Las Comunidades Europeas han realizado varios estudios tendientes a promover el desarrollo del EDI (Intercambio Electrónico de Datos) y el comercio electrónico. La primera etapa de estos estudios, incluyó un estudio sobre los obstáculos jurídicos al utilizar el EDI y se publicaron documentos sobre distintos aspectos del comercio ligado al documento electrónico, logrando en 1994 que se publicara el Modelo Europeo de Acuerdo EDI.

En una segunda etapa, se logra publicar en abril de 1997, la Iniciativa Europea de Comercio electrónico, fijando un objetivo claro,

la creación para el año 2000 de un marco jurídico coherente a escala europea en materia de comercio electrónico.

La cual va dirigida a fomentar el comercio electrónico en los aspectos de tecnología e infraestructura, a solventar cuestiones jurídicas y de reglamentación para generar confianza en los mecanismos de pago, en la protección de la propiedad intelectual e industrial y de los datos personales, garantizar una fiscalidad transparente y neutra con respecto al comercio tradicional evitando regulaciones divergentes en el marco internacional. También se pretende facilitar un entorno empresarial favorable, educando a los consumidores y empresas sobre las ventajas que ofrece.

Con el transcurso del tiempo se van desarrollando diversas propuestas, como la dirigida a establecer un marco común para la firma electrónica, la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, las cuales logran afectar aspectos esenciales del marco jurídico de referencia.

Pero es hasta octubre de1.997 que se lanza una comunicación hacia un marco europeo para la firma digital y cifrado, construyéndose de está forma los pilares de una ley que deberá irse

modificando y adecuando, como una figura que apenas se empieza a surgir.

Es así como empiezan a surgir proyectos de colaboración entre la Unión Europea y otros países como el proyecto piloto "Mercado Global para Pymes", coordinado por la Comisión Europea, Estados Unidos y Japón, que tiende a impulsar todo un conjunto de debates encaminados a mejorar la coordinación internacional, en los temas que afecten al desarrollo del comercio electrónico a escala mundial.

Es el 17 de setiembre de 1999, que nace a la vida jurídica "El Real Decreto-Ley 14/1999[63], dentro del cual se dispone una serie de regulaciones al uso de los certificados electrónicos, firma electrónica, firma electrónica avanzada o como hemos llamado comúnmente en el desarrollo de la presente investigación firma digital.

Reconociendo de esta forma "su eficacia jurídica y la prestación al público de servicios de certificación (Art. 1). Establece definiciones técnicas sobre la materia (Art. 2)"[64]

Confiriéndole en su artículo 3, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel, la cual será

[63] Dr. Agustín Viguri Perea, Catedrático de la Universidad Jaume I, España, Seminario sobre "La Firma Digital en la Función Notarial y Registral" Universidad de Costa Rica, Facultad de Derecho, jueves 5 de diciembre de 2002.

[64] Licda. Pérez Porta, Informe Técnico, Proyecto de Ley "Ley de Firma Digital y Certificados Digitales", Expediente 14276, Asamblea Legislativa, marzo de 2003.

admisible como prueba para juicio, según los criterios de apreciación establecidos en las normas procesales.

Bajo un régimen de libre competencia, donde la prestación de servicios de certificación no se encuentran sujetos a autorización previa, esto bajo los principios de objetividad, transparencia y no discriminación. (Art. 4).

No obstante a pesar de su carácter voluntario que brinda seguridad y protección de los derechos de los usuarios, determina y exige condiciones mínimas, que deberán cumplir los prestadores de servicios de certificación en el desempeño de su labor. (Art.6, 7 y 11).

Es importante analizar que este Real Decreto no sólo le abre las puertas a instituciones privadas, sino que a su vez regula el panorama de empleo de la firma electrónica a las Administraciones Públicas, brindándole autorización expresa al Estado para su uso. (Art. 6).

En resumen este Real Decreto establece una regulación clara del uso de la firma digital, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación.

De igual modo, este Real Decreto-ley determina el registro en el que deberán de inscribirse los prestadores de servicios de certificación, así como "el régimen de inspección administrativa de su

actividad, regula la expedición y la pérdida de eficacia de los certificados y tipifica las infracciones y las sanciones que se prevén para garantizar su cumplimiento."[65]

Es así como se da paso, al más reciente aporte jurídico del Parlamento Europeo, la Ley 34/2002, del 11 de julio, denominada Servicios de la Sociedad de la Información y de Comercio Electrónico.[66]

La anterior ley tiene como objetivo "la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de información." (Art. 1 Ley 34/2002).

---

[65] Dr. Agustín Viguri Perea, Catedrático de la Universidad Jaume I, España, Seminario sobre "La Firma Digital en la Función Notarial y Registral" Universidad de Costa Rica, Facultad de Derecho, jueves 5 de diciembre de 2002.

[66] Dr. Agustín Viguri Perea, Catedrático de la Universidad Jaume I, España, Seminario sobre "La Firma Digital en la Función Notarial y Registral" Universidad de Costa Rica, Facultad de Derecho, jueves 5 de diciembre de 2002.

Denominado sociedad de información a la expansión de las redes de telecomunicaciones y sobre todo de Internet, como vehículo de transmisión e intercambio de todo tipo de información, al incorporarse a la vida económica y social lo cual genera muchas ventajas tales como la eficiencia empresarial, el incremento de posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.

La ley se aplica con carácter general, a los prestadores de servicios establecidos en España, entendiéndose como establecimiento "el lugar desde el que se dirige y gestiona una actividad económica, definición compatible con la noción material de establecimiento predicado por el Derecho comunitario. La ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de información a través de un "establecimiento permanente" situado en España."[67]

Dispone esta ley en su artículo 2 inciso 3 que se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se ha inscrito en el Registro

[67] Dr. Agustín Viguri Perea, Catedrático de la Universidad Jaume I, España, Seminario sobre "La Firma Digital en la Función Notarial y Registral" Universidad de Costa Rica, Facultad de Derecho, jueves 5 de diciembre de 2002. folleto Pág.2 de 24.

Mercantil o en otro Registro Público español, con lo cual adquiera personalidad jurídica.

Asimismo, establece responsabilidades y obligaciones que deberán tener los prestadores de servicios al realizar actividades de intermediación como transmisión, copia, alojamiento y localización de los datos en la red.

Dentro de los intereses que presenta esta ley encontramos su afán por proteger los intereses de los destinatarios de servicios, dándoles garantías a la hora de contratar un servicio o bien por medio de Internet.

La ley promueve la elaboración de códigos de conducta, como instrumento de autorregulación, paralelo a esto brinda un medio de resolución alternativa de conflictos como lo es el arbitraje, con el fin de desaparecer las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de información.

La base de los principios que alude a esta ley como instrumento jurídico de aplicación obligatoria son: salvaguardar el orden público, la investigación penal, la seguridad pública y la defensa nacional, la protección de la salud pública, el respeto, la dignidad de la persona,

la no discriminación y la protección de la juventud y de la infancia, los cuales se encuentran consignados de una mejor forma en su artículo 8.

Finalmente se establece un régimen sancionador que clasifica las infracciones en muy graves, graves y leves, según corresponda.

Algunas de las iniciativas que ha tenido España, sobre el comercio electrónico con el pasar de los años son:

La Asociación Española de Comercio Electrónico (AECE), mayo de 1998; grupo de empresas españolas que intentan unificar esfuerzos con el fin de obtener un comercio electrónico más fiable y seguro.

El Commerce Net Español, es un consorcio para el uso, promoción y construcción del comercio electrónico en Internet.

El Consejo Superior de Cámaras de Comercio, Industria y Navegación de España, que representa en el ámbito nacional e internacional, a las 85 Cámaras de Comercio existentes en España, ha realizado algunas actuaciones dentro del entorno económico de las empresas.

Las iniciativas van dirigidas hacia la adopción de normas reguladoras sobre todo, en el aspecto de la seguridad en las comunicaciones ligadas a la firma electrónica y su valor jurídico.

La Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE), fundación que está integrada por el Consejo General del Notariado de España, el Consejo General de los Colegios de Corredores de Comercio de España, el Consejo General de la Abogacía de España, la Universidad de Zaragoza y la Sociedad Intercomputer S.A, entre los numerosos fines que tiene, incluye los de realizar estudios y proyectos sobre los mecanismos e instrumentos de seguridad que son necesarios para el desarrollo y utilización de las tecnologías de la información y la comunicación y colaborar al diseño de un marco legal que sea adecuado para realizar la certificación de transacciones electrónicas mantenidas entre la industria, el comercio, la banca, la Administración y los ciudadanos.

La Agencia de Certificación Electrónica (ACE), que tiene como objetivo principal la emisión de certificados para utilizar con el protocolo de pago electrónico SET.

CERES (Certificación Pública de Transacciones Electrónicas), es una autoridad de certificación pública desarrollada por la Fábrica Nacional de Moneda y Timbre. Además de la Fábrica, colaboran en CERES, el Ministerio de Administraciones Públicas, que participa en los grupos de trabajo técnico y jurídico encargados de desarrollar la

infraestructura técnica y el soporte legal a las operaciones de la autoridad de certificación, así como Correos y Telégrafos, encargado del sistema de registro de usuarios

Se intenta extender la actuación de la Fábrica Nacional, cuyo papel tradicional, ha sido el garantizar la seguridad de los documentos físicos, a los documentos y transacciones electrónicas realizadas entre ciudadanos o empresas y las Administraciones públicas, siendo el objetivo principal de CERES, el garantizar a ciudadanos y Administraciones la identidad de ambos participen en una comunicación, así como la confidencialidad e integridad del mensaje enviado, teniendo en cuenta que la información privada del usuario se encuentra almacenada en una tarjeta inteligente, protegida por un número de identificación personal, similar a la clave de una tarjeta de crédito. Este sistema puede utilizarse, por ejemplo, para garantizar la seguridad en la solicitud de diversos certificados (Registro Civil, Seguridad Social, etc.), y en general, para cualquier envío y recepción del documento oficial.

b.- INICIATIVAS ESTADOUNIDENSES.

Su inicio en este tema de investigación data de finales de la década de los setenta, cuando el gobierno de los Estados Unidos

publicó el Data Encryption Standard (DES) para sus comunicaciones de datos sensibles pero no clasificados.

Pero es hasta el 16 de abril de 1993, que el gobierno de los EE.UU. anunció una nueva iniciativa criptográfica encaminada a brindar a los usuarios un alto nivel de seguridad en las comunicaciones: "proyecto Clipper". Esta iniciativa según José Cuervo, en su trabajo jurídico sobre firma digital,[68] está basada en dos elementos fundamentales:

Un chip cifrador a prueba de cualquier tipo de análisis o manipulación (el Clipper chip o EES (Escrowed Encryption Standard) y

Un sistema para compartir las claves secretas (KES -Key Escrow System) que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.

Entre muchos países, es EE.UU. donde más se avanzada en este tipo de legislación sobre firma electrónica, sin embargo existen entidades que no lo consideran así tales como el Instituto Nacional de Ciencia y Tecnología, NIST (The National Institute of Science and Technology).

[68] José Cuervo, Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

El NIST ha introducido dentro del proyecto Capstone, el DSS (Digital Signature Standard) un estándar de firma, que todavía el gobierno americano no ha aprobado como estándar su utilización. El NIST se ha pronunciado a favor de la equiparación de la firma manuscrita y la digital.

La ley patrón o modelo de referencia para aplicar la firma digital, en Estados Unidos, según la ABA (American Bar Association o en español Asociación Americana), es **Digital Signature Guidelines** traducida al español como **"Ley de modelo de Firma Digital"**, de 1 de agosto de 1996.

La legislación y el valor probatorio de la firma ha sido ya admitido en Utah, primer estado en dotarse de una Ley de firma digital.

Esta fue aprobada el 27 de febrero de 1995 y modificada en diciembre de 1996, la firma digital de Utah **(Digital Signature Act Utah)**[69] se basa en un "Criptosistema Asimétrico" definido como un algoritmo que proporciona una pareja de claves segura.

Sus fines se establecen en el preámbulo de esta ley, los cuales son:

[69] Ley del Estado de Utah Sobre La Firma Digital, Código Comentado, Título 46, Capítulo 3 (1996), www.cnv.gov.ar/FirmasDig/Internacional/utah

1. Facilitar las transacciones mediante mensajes electrónicos confiables;

2. Reducir al mínimo la posibilidad de fraguar firmas digitales y el fraude en las transacciones electrónicas;

3. Instrumentar jurídicamente la información de norma pertinentes de la Unión Internacional de Telecomunicaciones, y

4. Establecer, en coordinación con diversos Estados, normas uniformes relativas a la autenticación y confiabilidad de los mensajes electrónicos.

La Ley del Estado de Utah define la firma digital como la transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza:

Si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectúo la transformación.

Esta ley le da a la firma digital el mismo efecto legal que una firma manuscrita, no obstante la firma digital deberá cumplir con ciertas existencias; "una de las exigencias es que la firma digital sea verificada por referencia a una clave pública incluida en un

certificado válido emitido por una autoridad de certificación con licencia."[70]

Otra de las iniciativas del Estado de Utah fue en 1997 redactar un proyecto de ley **(The Act on Electronic Notarization).**

El Estado de California define "la firma digital como la creación por ordenador de un identificador electrónico que incluye todas las características de una firma válida, aceptable, como: única, capaz de comprobarse, bajo un solo control, enlazándose con los datos de tal manera que si se cambian los datos se invalide la firma…"[71]

Dentro de otras iniciativas que el señor José Cuervo hace en su trabajo anteriormente mencionado podemos hacer referencia en orden cronológico a las siguientes:

2 de agosto de 1994, la **ABA,** da a conocer la **"Resolution Concerning the CyberNotary: an International Computer-Transaction Specialist"** cuya traducción libre al español es Resolución referente al Notario Cibernético: Especialistas Internacionales en transacciones por medio del computador.

---

[70] José Cuervo, Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

[71] José Cuervo, Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

Mayo de 1.996, **The Electronic Signature Act Florida,** que reconoce la equivalencia probatoria de la firma digital con la firma manual. En esta ley existe un cambio significativo en comparación con otras leyes que es la utilización del término "international notary" traducido al español como notario internacional, en vez del "cybernotary" o notario cibernético, utilizado en otras leyes de EE.UU.

30 de mayo de 1997, **The Electronic Commerce Act**, que hace referencia al cybernotary.

En el año 1996, **The Massachusetts Electronic Records and Signatures Act**, acoge todo mecanismo capaz de proporcionar las funciones de las firma manuscrita sin ceñirse a un tipo concreto de tecnología.

c.- INICIATIVAS ALEMANAS.

Dentro de la legislación alemana nos encontramos con la Ley de Firmas Digitales aprobada por el Bundestag el día 13 de junio de 1997, la cual forma parte integral de una Ley más amplia denominada Ley Multimedia.

Ambas pretenden regular con carácter general las condiciones de los servicios de información y documentación.

No obstante La Ley de firmas digitales, empieza por hacer cuatro definiciones básicas: firma digital, certificador (firma digital y atributos), certificado y sello temporal.

Firma digital: sello de datos digitales creado por una llave privada que permite determinar a través de la llave pública asociada a ella y determinada en un certificado, quien es el titular de la firma y que los datos firmados no han sido alterados.

Certificador: persona física o jurídica que atestigua la atribución de una llave pública a una persona física, disponiendo para ello de la correspondiente licencia.

Identificando dos tipos de certificados: de firma digital y de atributos.

Certificado de firma digital: testimonio relativo a la atribución de una llave pública a una persona física, a la que se asocia una firma digital.

Certificado de atributos: testimonio especial digital en el que se contienen datos adicionales sobre el mismo.

Sello temporal: testimonio digital expedido por un certificador, que tiene unida una firma digital.

Establece un marco para la utilización de las firmas digitales, exigiendo la obtención de un certificado de firma digital previo a utilizar la firma digital.

Obligando a su vez a los certificadores a obtener antes de brindar el servicio una licencia que deberá solicitar a la Autoridad, para así de esta forma lograr una protección favorable hacia los usuarios.

La Ley impone al certificador un cierto deber de información y de asesoramiento al solicitante del certificado.

El artículo 6 de la Ley establece un deber de asesoramiento por lo que el certificador deberá advertir al solicitante, de acuerdo con el artículo 5 párrafo 1, las medidas necesarias para contribuir a dar seguridad a las firmas digitales y a su verificación fiable.

El artículo 7, regula el contenido de los certificados que deberán tener como mínimo el nombre del titular de la firma llave pública, al que deberán añadirse una anotación adicional si hay posibilidades de confusión, una llave pública atribuida, un algoritmo con el que la llave pública del titular, así como la llave pública del certificador puede usarse, el número del certificado, el inicio y final de la validez del

certificado, el nombre del certificador y la información sobre si el uso de la firma digital está limitado a aplicaciones determinadas.

En este mismo artículo 7, la información relativa al poder de representación de un tercero, o a la profesión u otra titulación.

El artículo 13 regula el control y exigencia de responsabilidades, en ese sentido la Autoridad, podrá tomar las medidas en relación a los certificadores para asegurar el cumplimiento de esta Ley, asimismo permitirá a la Autoridad el acceso a sus establecimientos y locales, teniendo en cuenta que en el supuesto de incumplimiento de las obligaciones derivadas de la Ley, la Autoridad deberá revocar tal licencia.

Por último, hace referencia, a los certificados extranjeros en conexión con las firmas digitales que puedan ser comprobadas con una llave pública que haya sido certificada por otro Estado Miembro de la Unión Europea o por otro Estado firmante del Tratado del Área Económica, previendo la Ley, la autorización al Gobierno Federal para promulgar mediante Reglamento, las disposiciones necesarias para desarrollar los artículos de la misma.

Es importante observar que uno de los puntos más importantes de esta Ley es el control de la Autoridad con respecto a los

certificadores, solicitándole una concesión de licencia por parte de la Autoridad, además de mantener por parte de la Autoridad una supervisión constante sobre los mismos al margen de la ley.

El proyecto de Reglamento de firmas digitales, de la Ley alemana de dichas firmas, establece un desarrollo más detallado en su artículo 3 sobre la solicitud de certificados, incluyendo a los largo del proyecto diferentes puntos sobre la creación y custodia de llaves de firmas y claves de identificación, la validez de los certificados la cual no podrá ser superior a 5 años, los Registros Públicos de certificados, el control de los certificados entre otros puntos más.

d.- INICIATIVAS DE NACIONES UNIDAS.

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL) en su 24º periodo de sesiones celebrado en el año 1991, acordó encargar a un grupo de trabajo el estudio de los problemas jurídicos del intercambio electrónico de datos (EDI: Electronic Data Interchange) .

El Grupo de Trabajo se dedicó del 27 de enero al 7 de febrero de 1992, a este tema y elaboró un informe que fue elevado a la Comisión.

Dicho informe examina la definición de "firma" y otros medios de autenticación que se han dado en algunos convenios internacionales. Teniendo siempre en cuenta la definición amplia de "firma" que se contiene en la Convención de las Naciones Unidas sobre Letra de Cambio Internacionales y Pagarés Internacionales, que dice: "El término firma designa la firma manuscrita, su facsímil o una autenticación equivalente efectuada por otros medios"[72].

En su 25º período de sesiones celebrado en 1992, la Comisión examinó el informe del Grupo de Trabajo y encargó la preparación de la reglamentación jurídica del EDI al Grupo de Trabajo, dedicándose este grupo a establecer un equivalente funcional a la firma digital que tuviera validez legal.

Aprobando El Plenario de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL), el 14 de Junio de 1996 en su 29º periodo de sesiones celebrado en Nueva York, el proyecto de Ley Modelo sobre aspectos jurídicos de EDI (Resolución General de la Asamblea 51/162 de 16 de diciembre de 1996).

[72] José Cuervo, Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

No obstante es hasta en su 37º período de sesiones, del 18 al 29 de setiembre de 2000, celebrado en Viena, que se aprobó la **"Ley Modelo de la CNUDMI para las firmas electrónicas".**

La Ley Modelo se preparó "partiendo del supuesto de que debería derivarse directamente del artículo 7 de la Ley Modelo de la CNUDMI sobre comercio electrónico y considerarse como una forma de proporcionar información detallada sobre el concepto del "método fiable para identificar" a una persona y "para indicar que esa persona aprueba" la información que figura en el Mensaje de datos."[73]

El artículo 7 de la Ley Modelo sobre Comercio Electrónico (LMCE)[74] regula el equivalente funcional de firma, estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos, que nos da un concepto amplio de firma electrónica,

[73] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Asamblea General de las Naciones Unidas, 34º período de sesiones Viena, 25 de junio a 13 de julio 2001, distribuido 17 de mayo de 2001 en Español, 32

74 Ley Modelo de la CNUDMI , 1996, Artículo 7.- Firma.-1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; yb) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.3) Lo dispuesto en el presente artículo no será aplicable a: [...].

indicando "cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) si ese método es tan fiable como sea apropiado para los fines para los que se creó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acto pertinente".

Entre algunos de los objetivos fundamentales para promover la economía y la eficacia del comercio internacional figuran el facilitar o permitir el empleo de firmas electrónicas y el de conocer igualdad de trato a los usuarios de documentación consignada en papel y soporte informático.

"La finalidad de la Ley Modelo no es obstaculizar la vigencia de las normas de derecho internacional privado. A diferencia de un convenio o convención internacional, la ley modelo no requiere que el Estado promulgante notifique a las Naciones Unidas o a otros Estados que asimismo puedan haberlo promulgado."[75]

[75] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Asamblea General de las Naciones Unidas, 34º período de sesiones Viena, 25 de junio a 13 de julio 2001, distribuido 17 de mayo de 2001 en Español, Pág. 20.

No obstante lo anterior, las Naciones Unidas recomiendan a los Estados que informen a la Secretaría de la CNUDMI, la promulgación de la ley.

Una de las características importantes que tiene esta ley es que al ser incorporada al derecho interno de cada Estado, se puede adecuar a las necesidades propias, excluyendo o modificando algunas de sus disposiciones, por lo que le da un carácter de flexibilidad inherente.

Esto siempre y cuanto se incorpore a su derecho interno los "principios básicos neutralidad tecnológica, no discriminación entre firmas electrónicas nacionales y extranjeras, la autonomía de las partes y el origen internacional de la Ley Modelo."[76]

Es importante mencionar que la Ley Modelo es considerada un instrumento jurídico independiente, esto se debe a que cuando se terminó la confección de la misma ya se había aplicado de manera satisfactoria y eficaz en una serie de países y en otros estaban estudiando su aprobación.

A su vez, la Ley Modelo no abarca en detalle lo referente a la responsabilidad que puedan tener cada una de las partes interesadas

[76] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Asamblea General de las Naciones Unidas, 34º período de sesiones Viena, 25 de junio a 13 de julio 2001, distribuido 17 de mayo de 2001 en Español, Pág. 21

en el funcionamiento de los sistemas de creación de firmas electrónicas, estas consideraciones las deja abiertas al margen del derecho que sea aplicable. Sin embargo se fijan criterios para evaluar la conducta de las partes.

Ante la evolución de las innovaciones tecnológicas, la Ley Modelo, no abarca todos los aspectos del empleo de firmas electrónicas, por el contrario establece criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología que se utilice ya sean firmas electrónicas basadas en la criptografía asimétrica, los dispositivos biométricos (que permiten la identificación de personas por sus características físicas como geometría manual o facial, huellas dactilares, retina, reconocimiento de voz), la utilización de contraseñas, versiones digitalizadas de firmas manuscritas, entre otros.

La Ley modelo establece que el lugar de origen no debe ser un factor para determinar si puede reconocerse la capacidad o validez de los certificados extranjeros o las firmas electrónicas, para tener eficacia jurídica en un Estado, sino que su determinación se derive del grado de fiabilidad técnica que se posea en uno u otro.

En el marco de actividades de formación y asistencia, tenemos que tener presente que la Secretaría de la CNUDMI, brinda asistencia a los Estados, para la preparación de la legislación que se base en la Ley Modelo de la CNUDMI para las firmas electrónicas.

Otra organización importante que se ha pronunciado al respecto es la OCDE (Organización para la Cooperación y Desarrollo Económico) sobre la utilización de criptografía (Guidelines for Cryptography Policy), la cual fue aprobada el 27 de marzo de 1997.

A pesar de que esta recomendación no es vinculante, señala una serie de reglas que los gobiernos debieran tener en cuenta al adoptar legislación sobre firma digital y terceros de confianza, con el fin de impedir la adopción de diferentes reglas nacionales que podrían dificultar el comercio electrónico y la sociedad de la información en general.

e.- INICIATIVAS EN OTROS PAÍSES

En Francia

Nueva Ley de Telecomunicaciones y disposiciones sobre uso interior de cifrado.

En Italia

La Ley de 15 de marzo de 1997 número 59, es la primera norma del ordenamiento jurídico italiano que recoge el principio de la plena validez de los documentos informáticos.

El reglamento aprobado por el Consejo de Ministros el 31 de octubre de 1997, reconoce del valor jurídico del documento informático de las firmas digitales

Define la firma digital como "el resultado del proceso informático (validación) basado en un sistema de claves asimétricas o dobles, una pública y una privada, que permite al suscriptor transmitir la clave privada y al destinatario transmitir la clave pública, respectivamente, para verificar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos (artículo 1° apartado b). En el reglamento la firma digital está basada exclusivamente en el empleo de sistemas de cifrado llamados asimétricos."[77]

En el artículo 2 del Reglamento italiano hace la mención a que los documentos informáticos serán válidos y eficaces a todos los efectos legales si son acordes a las exigencias del Reglamento.

[77] José Cuervo, Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp.

Estableciéndose en el artículo 10.2 la equiparación de la firma digital sobre un documento informático a la firma escrita en soporte papel.

El artículo 11.1 establece concordado con el artículo 2 del Reglamento italiano, que los contratos realizados por medios telemáticos o informáticos que utilicen la firma digital según las disposiciones del reglamento serán válidos y eficaces a todos los efectos legales. No obstante tendrá que tenerse en cuenta el artículo 8, el cual establece que cualquiera que pretenda utilizar la criptografía asimétrica con los efectos del artículo 2 debe conseguir un par de claves adecuadas y hacer pública una de ellas a través del procedimiento de certificación mediante un certificador.

La Ley y el Reglamento regulan a su vez la validez del documento informático; el documento informático sin firma digital; el documento informático con firma digital; los certificadores; los certificados; autentificación de la firma digital; el "cybernotary"; los actos públicos notariales; la validación temporal; la caducidad, revocación y suspensión de las claves; la firma digital falsa; la duplicidad, copia y extractos del documento; y la transmisión del documento.

En Reino Unido

"Hay un vivo debate sobre la posible reglamentación de los Terceros de Confianza -TC. Existe un proyecto de ley sobre firma digital y Terceros de Confianza."[78]

En Dinamarca, Suiza y Bélgica

Preparan proyectos de ley sobre firma digital.

En Panamá, Guatemala, Argentina, Venezuela, Colombia

Ya poseen ley que regula la firma digital.

SECCIÓN SEGUNDA: DESARROLLO DE LA FIRMA DIGITAL EN COSTA RICA.

a.- COMENTARIOS GENERALES AL PROYECTO DE LEY NÚMERO 14276.

El proyecto de ley que viene hacer base fundamental para desarrollar la presente investigación, ha sido denominado "Ley de Firma Digital y Certificados Digitales, expediente número 14276, publicado en el Diario Oficial la Gaceta número 82 del 30 de abril de 2001.

El proyecto consta de cuatro títulos, compuestos los dos primeros títulos por tres capítulos cada uno y los dos últimos títulos

[78] José Cuervo, Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

poseen un capítulo único cada uno, para un total de veinte artículos que se desarrollan a lo largo del documento.

Dicho proyecto surge a raíz de los grandes avances que se han venido descubriendo en materia de comunicación con el Internet, la cual ha ampliado las facilidades de comunicación entre los seres humanos, construyendo un canal de flujo ideal.

Cada vez los expertos y las mismas empresas coinciden en que gracias a esta útil herramienta de trabajo, de diversión, comunicación, etc., es que se ha abierto la posibilidad de un acceso ilimitado de información y una posibilidad de competencia hacia los mercados mundiales.

Esto se debe a los grandes atributos que Internet da a todos como lo son la transmisión rápida, el bajo costo de sus servicios, su eficiencia y su desarrollo en todos los territorios y países del mundo logrando romper barreras inimaginables.

Es así como en Costa Rica nace la idea de regular las transferencias electrónicas, que utilicen el Internet por medio de la firma digital o firma electrónica avanzada, sin limitar por esto el uso de nuevas tecnologías que puedan desarrollarse con el pasar del tiempo.

Dándoles a los usuarios más seguridad y protección al realizar todo tipo de transacciones, que se regulan mediante un marco jurídico determinado y aprobado en nuestro país.

El objetivo del Proyecto de Ley es "dar validez jurídica a la firma digital y autorizar al Estado para su utilización. (artículo 1)"[79]

Aunque el Tribunal Supremo de Elecciones, ha sido mucho más especifico en su informe del proyecto de ley solicitado por la Asamblea Legislativa afirmando que: "El proyecto tiene como objeto regular el uso y reconocimiento jurídico de la firma digital, otorgándole la misma validez y eficacia jurídica que a una firma manuscrita y otra análoga que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización. Para tales efectos, se regula el reconocimiento legal expreso de la firma digital avanzada, se determinan sus normas de acreditación y sus efectos jurídicos, se eleva a rango legal el "principio de equivalencia funcional"-que otorga al documento digital firmado el mismo valor del documento

[79] María Teresa Bermúdez, Adolfo Barquero, Danilo Retana y Ana Lucía Jiménez, Informe a la Dirección General del Archivo Nacional respecto a la posición tomada hacia el proyecto de ley 14276, Asamblea Legislativa Expediente 14276, folio 47

escrito-, se acoge el "principio de neutralidad tecnológica"-a fin de no limitar el mecanismo de la firma digital a una sola tecnología- …"[80]

En el artículo 2 del citado proyecto se definen veinticuatro términos necesarios para la comprensión del mismo algunos de los más importantes son: certificado digital, certificado digital reconocido, documento, firma digital, firma digital avanzada, intermediario, mensaje de datos, procedimiento seguro, receptor, signatario, entre muchos otros.

A su vez define las entidades encargadas de regular dicha validez y autorizar su utilización, designa como **Órgano rector** al Ministerio de Ciencia y Tecnología, el cual además de sus funciones le compete las decisiones técnicas, las **Autoridades de Acreditación** deberán estar afiliadas o adscritas al Ministerio de Ciencia y Tecnología cuyas funciones son evaluar a los solicitantes, autorizar a los prestadores de servicios de certificación, registrar e inspeccionar las entidades y los **Prestadores de Servicios de Certificación** que van a ser las personas físicas o jurídicas que emiten certificados, cualquier persona autorizada y competente. (Art. 8, 13, 14, 15, 16).

[80] Oscar Fonseca, Presidente del Tribunal Supremo de Elecciones, Informe del Proyecto de Ley 14276 a la Asamblea Legislativa, Expediente 14276, folio 269

Artículo 5, concede a la firma digital cuando ha cumplido con una serie de requisitos el mismo valor jurídico que la firma manuscrita en relación con la firma consignada en papel.

Artículo 7, autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, Contraloría General de la República, Defensoría de los Habitantes, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales para la utilización de la Firma Digital Avanzada.

Los artículos que van del 10 al 12, vinculan y regulan lo concerniente a los certificados digitales desde los requisitos mínimos necesarios que deberán tener, los motivos por los que podrán ser cancelados y revocados, hasta establecer la equivalencia de los certificados emitidos por entidades no establecidas en Costa Rica.

Al final de este proyecto se dedica estipular los requisitos que deberán cumplir los dispositivos seguros de creación de la Firma Digital, la forma en que deberán de verificarse dichos dispositivos, sin embargo no prohíbe la existencia de convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos, obligaciones, y al mismo tiempo las condiciones técnicas y de cualquier clase.

En las disposiciones finales de dicho proyecto que se encuentra adjunto a esta investigación, se establece que El Poder Ejecutivo deberá emitir el reglamento a la presente ley dentro del plazo máximo de tres meses siguientes a su publicación, artículo que a pesar de ser el último no deja de ser importante, debido a que deberá regular muchos puntos importantes presentes en esta ley, pasando a ser el reglamento un texto esencial para la implementación de la firma digital.

b.- ESTADO DEL PROYECTO DE LEY 14276.

En principio este proyecto se pasó a estudio e informe de la Comisión Especial de Propiedad Intelectual.

Para luego solicitar el estudio, propuestas y comentarios de distintas instituciones tanto públicas como privadas acerca de la trascendencia y aplicación de este proyecto, algunas de las instituciones que se pronunciaron y expresaron sus comentarios fueron:

- **Dirección General de Archivo Nacional[81]:** el 28 de mayo del 2001 presenta sus observaciones y comentarios a la Asamblea Legislativa, haciendo énfasis en el criterio negativo que

[81] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir Departamento de Asuntos Jurídicos y solicitar el expediente 14276, ver los folios 36-50.

produciría la aprobación del proyecto como fue presentado a la Asamblea Legislativa.

Dentro de las principales observaciones que hace la Dirección tenemos:

1. Se debe tener en cuenta el adecuado marco jurídico que tiene Costa Rica en la Ley 7202, Ley del Sistema Nacional de Archivos, que regula la creación, la organización y conservación de los documentos y los archivos de las Instituciones del estado.
2. Se debe tener cuidado, a la hora de autorizar a todas las Instituciones del Estado Costarricense sin especificar requisitos, responsabilidades o sanciones por su mala utilización.
3. Se debe asegurar el acceso y la conservación de los documentos que exige la Constitución Política a todos los ciudadanos.
4. Se deberá preparar profesional y presupuestariamente a todas la Instituciones del Estado de Costa Rica (Ministerios, Municipalidades, Direcciones Generales, Instituciones Descentralizadas y en general a todos los Poderes del

Estado), para asumir de forma responsable la administración de los documentos en soporte electrónico.

5. Se debe definir claramente el concepto documento electrónico.
6. Se debe resaltar las características propias de los documentos electrónicos.
7. Se debe regular el ciclo vital del documento electrónico, así como enumerar aspectos esenciales como concepción del documento, creación, mantenimiento, valoración, acceso y conservación del documento electrónico.
8. La firma digital y el documento electrónico deben ser tratados con mayor profundidad.
9. El título no coincide con el proyecto de ley, no regula el documento electrónico.
10. No establece ningún tipo de sanciones.
11. Hay conceptos muy amplios que originan confusión.
12. Se debe regular en forma específica el uso de la firma digital en la Administración pública.

- **Instituto Centroamericano de Administración Pública (ICAP)[82]:** el 22 de julio de 2001 presenta sus observaciones al respecto y pone en conocimiento algunos aspectos:
    1. Es importante darle la mayor difusión posible al proyecto ya que sus efectos recaen en la sociedad costarricense.
    2. Los conceptos que se utilizan son confusos, ambiguos e incluso se contradicen.
    3. Se debe definir las responsabilidades para los involucrados.
    4. Estipular las excepciones para la aplicación de la firma digital y certificados digitales.
    5. La autoridad certificadora no tiene claridad en cuanto a su naturaleza jurídica, composición y financiamiento.

- **Instituto Costarricense de Pesca y Agricultura (INCOPESCA)[83]:** realiza un breve resumen del proyecto, la meta del mismo, su

[82] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 51-52

[83] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 217-128.

objetivo primordial y vuelve a definir el Órgano rector. Este instituto manifiesta que no tiene objeción alguna al proyecto.

- **Compañía Nacional de Fuerza y Luz[84]:** el 4 de diciembre de 2001 manifiesta que esta de acuerdo con el presente proyecto de ley.
- **Banco de Crédito Centroamericano (BANCENTRO)[85]:** 5 de diciembre de 2001, informa que esta identificado con el proyecto.
- **Corporación Bañes S.A.[86]:** considera que existen en este proyecto algunos vacíos que crean problemas en cuanto al reconocimiento y la validez de la firma y los certificados digitales algunos son:
    1. No establece requisitos que deben tener las personas físicas o jurídicas que deseen inscribirse ante el Ministerio de Ciencia y Tecnología.

[84] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 224.

[85] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 227.

[86] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 223, 230.

2. No indica la manera en que se puede reconocer como válida la firma digital.
3. No se establece ningún procedimiento consular para este tipo de firmas certificadas, el banco debe tener estricta certeza sobre los documentos y las firmas que solicitan o autorizan transacciones.
4. En el reglamento se debe establecer mecanismos técnicos, recursos y personal capacitado para que ejerza esas funciones.
5. No define claramente el término certificado digital.
6. Deja en entre dicho si la cancelación o revocación por causa de expiración del plazo, acarrearía una nulidad e inexistencia posterior de ese contenido.
7. Sugiere que se establezca un procedimiento para la cancelación o revocación de las firmas.
8. Se deben hacer reformas al Código Procesal Penal y al Código Procesal Civil, de manera que indique que la firma digital y los certificados digitales pueden ser medios probatorios.

9. Se debe tutelar la confidencialidad de las informaciones y los procedimientos.

- **Registro Nacional de Costa Rica[87]:** el 6 de diciembre de 2001 expone su criterio respecto al proyecto. Considera que:

1. Se deben preparar normas uniformes sobre las firmas digitales y las entidades certificadoras.
2. Regular en forma clara lo referente al documento electrónico y su validez.
3. Se debe determinar la relación entre el contenido del documento electrónico y el soporte en que va a estar, para asegurar la información de manera confiable, autentica y apta para ser conservada.
4. Se debe tener la tecnología y métodos para la prevención de errores.
5. Longetividad del soporte.
6. Respaldos necesarios.
7. Los conceptos en el proyecto son ambiguos y confusos.

[87] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 231-234.

8. Se debe definir las responsabilidades de los entes involucrados.
9. Estipular excepciones a la utilización de la firma digital.

- **Ministerio de Industria y Comercio[88]:** el 22 de marzo del 2002 entrega las observaciones, en las cuales hace un análisis jurídico del articulado del proyecto en el cual difiere sobre todo en aspectos de redacción y de forma.
- **Junta de Protección Social de San José[89]:** esta institución considera que sería de gran utilidad para la Administración Pública el utilizar la tecnología electrónica en las diferentes comunicaciones.
- **Superintendencia General de Entidades Financieras (SUGEF)[90]:** considera importante el proyecto en materia de uso de la tecnología de información y telecomunicaciones, catalogando la aprobación de esta ley como urgente

[88] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 233-241.

[89] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 242.

[90] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 254-256.

debido a que algunos proyectos en curso demandan la vigencia de su contenido tales como: Servicio de Información Confidencial, Envío por parte de las entidades supervisadas a la SUGEF de los datos e información que la normativa establece, Intercambio de la correspondencia oficial, Acceso remoto a la red interna de la SUGEF.

No obstante considera que el proyecto carece de algunos elementos en materias importantes como:

1. Requisitos, obligaciones y responsabilidades de las empresas con licencia para certificar.
2. Infracciones y Sanciones en especial para terceros.
3. Regulación en cuanto al cobro de comisiones para el reconocimiento de acreditación y certificaciones.
4. Riesgos de pérdidas ante eventuales problemas.

- **Banco de Costa Rica[91]:** no tiene objeciones al proyecto.
- **Ministerio de Hacienda, Dirección General de Aduanas[92]:** realiza un breve análisis al proyecto identificando las ventajas

[91] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 255.

[92] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 259-261.

que nos traería, asimismo considera que de aprobarse la ley deberán realizarse varias reformas que ya están estudiando. Al proyecto en general solo le hacen 3 observaciones:

1. La aprobación de la ley implicaría la revisión de los controles aduaneros, así como la operatividad de las determinadas gestiones aduaneras.
2. Se debe definir de manera más clara las competencias de la Autoridad de Acreditación.
3. Se debe estipular la jerarquía de los sujetos que participan y los distintos campos de acción.

- **Ministerio de Gobernación, Policía y Seguridad Pública**[93]: en el campo de este ministerio no tienen observaciones que hacerle al proyecto de ley.
- **Tribunal Supremo de Elecciones**[94]: realiza un breve análisis al proyecto identificando los objetivos del proyecto, la relevancia jurídica, la eficacia y necesidad que existe de aprobar este proyecto. No obstante sugiere que el artículo

[93] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 262.

[94] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 269-271.

sétimo se le incluya como institución autorizada, de lo demás no tiene objeciones.

- **Banco Nacional[95]**: realiza observaciones a los artículos 1, 2, 6, 7, 9, 11 inc. 6, 12, 13, 14, sobre definiciones de términos más claros, sugerencias para ampliar el texto de los artículos, acuerdos privados, cancelación y revocación, derechos de terceros, jerarquías y procesos a seguir.
- **Banco Popular y de Desarrollo Comunal[96]**: realiza un breve resumen del proyecto identificando claramente el propósito del mismo. No obstante considera que:

1. El proyecto no aclara donde se definirá el proceso y la naturaleza jurídica de las empresas que certifican.
2. Es importante señalar la protección al titular de la firma digital y por supuesto a las transacciones que este realice.
3. Se debe crear un Centro de registro e inscripciones de certificados digitales, que pueda llevar a cabo la misma Autoridad de Acreditación.

[95] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 273-277.

[96] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 285-289.

4. Se debe tener uniformidad dentro del texto para evitar la confusión.
5. Identificar las funciones y servicios que brindarán las empresas certificadoras.

- **Caja Costarricense del Seguro Social (CCSS)[97]:** el 4 de febrero comunica a la Asamblea Legislativa que está de acuerdo con este proyecto.
- **RACSA[98]:** considera que la aprobación y eficacia del proyecto son de beneficio para esta y las demás instituciones del estado. No obstante solicita que en el artículo 7, se le incluya dentro de las instituciones autorizadas.
- **Ministerio de Salud[99]:** expresa que a pesar de que no infiere dentro del resorte de esta cartera, si es importante tener en cuenta que: el uso de la firma digital y certificados digitales conlleva tener un dispositivo seguro de creación de la firma,

[97] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 290.

[98] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver el folio 291.

[99] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 292-293.

así como contar con personal de gran solvencia moral, se debe conocer los alcances y consecuencias en el ámbito nacional y personal y se tiene que tener en cuenta principalmente las arcas presupuestarias.

- **Ministerio de Comercio Exterior[100]:** el 11 de febrero de 2002 emite sus observaciones al proyecto y en especial a los artículos 1, 2, 5, 6, 7, 10 y 11, 13, 14, dentro de sus sugerencias encontramos:

1. Sería bueno eliminar toda mención a los documentos o a la certificación digital de documentos, dado que genera confusión.
2. Eliminar y aclarar ciertos términos como: certificado digital reconocido, procedimiento seguro, firma digital y firma digital avanzada, etc.
3. Dejar claro la actuación del notario.
4. Estipular el plazo de vigencia de los certificados y como operaran los plazos.

[100] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 306-310.

5. Se debe establecer un artículo donde se identifiquen las responsabilidades, obligaciones, deberes y derechos de las empresas certificadoras y de la autoridad acreditadota.
6. Se debe establecer normativa relacionada con las facultades de fiscalización de la Autoridad de Acreditación.

- **Patronato Nacional de la Infancia[101]:** considera que es muy acertado y oportuno que el legislador tome en cuenta autorizar al Estado en general, para la utilización de la firma digital y el uso de los documentos electrónicos firmados digitalmente.

Luego de todos estos pronunciamientos de diversas instituciones, se realiza el martes 5 de marzo de 2002, una sesión donde se le convoca al Máster Edwin Aguilar Sánchez, quien es máster en Ciencias de la Computación de la Universidad de Essex en Inglaterra, tiene especialización en Comercio Electrónico en la Organización Mundial del Comercio, OMC Ginebra Suiza, es Director de Tecnología de Información del ICAP, es investigador del Centro de Investigaciones en Computación del Instituto Tecnológico de Costa Rica y Profesor de Comercio Electrónico.

[101] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 322-323.

El señor Aguilar en esta sesión expone y aclara la figura de la firma digital por medio de ejemplos que facilitan la compresión del tema que se esta estudiando, ayudando a muchos de los licenciados a la comprensión del tema que se esta discutiendo y aprobando[102].

Asimismo, después de las múltiples sesiones realizadas para discutir y mejorar los artículos, tomando siempre en cuenta las observaciones de las instituciones y la ayuda del Máster Edwin Aguilar, se presenta el 13 de marzo de 2002 un texto sustitutivo al proyecto de ley 14276.

El texto sustitutivo[103] consta de seis capítulos y veintisiete artículos.

Después de esta fecha, se establece una comisión para que rindan un informe del texto sustitutivo y a su vez solicitan criterios, observaciones y mociones a las instituciones públicas y privadas.

[102] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 420-452.

[103] Si se quiere profundizar en los comentarios realizados por esta institución se puede acudir a el Asamblea Legislativa, Departamento de Asuntos Jurídicos, solicitar el expediente 14276 y ver los folios 571-581.

TÍTULO SEGUNDO

TÉCNICAS Y USOS DE LA FIRMA DIGITAL DENTRO DE LAS TRANSACCIONES COMERCIALES.

CAPÍTULO PRIMERO.

TÉCNICAS PARA LA UTILIZACIÓN DE LA FIRMA DIGITAL DENTRO DE LAS TRANSACCIONES COMERCIALES.

SECCIÓN PRIMERA: ELEMENTOS Y REQUISITOS PARA LA UTILIZACIÓN DE LA FIRMA DIGITAL.

a.- ELEMENTOS FORMALES.

Para utilizar en forma adecuada la firma digital, debemos tener en cuenta ciertos presupuestos que son parte esencial de la firma y que sin estos sería muy difícil su existencia. Algunos de estos son:

a.1- AUTORIDAD O ENTIDAD DE CERTIFICACIÓN: "son las encargadas de otorgar autenticación a firmas y certificados digitales generados por medios electrónicos, así como de precisar otros detalles como el plazo de su validez."[104]

Dentro del sistema de seguridad que indicamos, para que cualquier usuario pueda confiar en otro usuario se deben establecer

[104] DE PALADELLA SALORD (Carlos), El Dinero físico y su desaparición?, Argentina, 1999. Documento de Internet disponible: http://www.publicaciones.derecho.org/redi/index.cgi?/N%Famero_10_-Mayo_de 1999/paladella

ciertos protocolos. Los protocolos sólo especifican las reglas de comportamiento por seguir.

Según José Cuervo en "La Firma Digital y Entidades de Certificación"[105] expone que existen diferentes tipos de protocolos en los que intervienen terceras partes confiables (Trusted Third Party, TTP, en inglés):

Los **protocolos arbitrados.** En ellos una TPC o Autoridad de Certificación participa en las transacciones para asegurar que ambos lados actúan según las pautas marcadas por el protocolo.

Los **protocolos notariales.** En este caso la TPC, además de garantizar la correcta operación, también permite juzgar si ambas partes actuarán por derecho según la evidencia presentada a través de los documentos aportados por los participantes e incluidos dentro del protocolo notarial. En estos casos, se añade la firma (digital) del notario a la transacción, pudiendo éste testificar, posteriormente, en caso de disputa.

Los **protocolos autoverificables.** En estos protocolos cada una de las partes puede darse cuenta si la otra actúa deshonestamente, durante el transcurso de la operación.

---

[105] José Cuervo, http://www.informatica-juridica.com/trabajos/firma_digital.asp

En Costa Rica, estos protocolos deberán aplicarse según las necesidades que se presenten, debido a que la aplicación de uno no es excluyente a la aplicación de algún otro.

La Autoridad o Entidad de Certificación deberá reunir los requisitos que determine la ley, conocimientos técnicos y experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad.

El documento WP.71 de 31 de diciembre de 1.996 de la Secretaría de las Naciones Unidas indica en su párrafo 44 que las entidades certificadoras deben seguir criterios de:

- Independencia.
- Recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida.
- Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.
- Longevidad.
- Aprobación del equipo y los programas.
- Mantenimiento de un registro de auditoria y realización de auditorias por una entidad independiente.

- Existencia de un plan para casos de emergencia (programas de recuperación en casos de desastres o depósitos de claves).
- Selección y administración del personal.
- Disposiciones para proteger su propia clave privada.
- Seguridad interna.
- Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.
- Garantías y representaciones (otorgadas o excluidas).
- Limitación de la responsabilidad
- Seguros
- Capacidad para intercambiar datos con otras autoridades certificadoras.
- Procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado expuesta).

Hugo Daniel Carrión, en su análisis comparativo de legislación y proyectos manifiesta que:[106]

[106]Hugo Daniel Carrion, http://www.informatica-juridica.com/trabajos/analisis_comparativo_a_nivel_mundial_sobre_firma_digital.asp

"Un certificado digital es un fichero digital intransferible y no modificable, emitido por una tercera parte de confianza (Autoridad de Certificación), que asocia a una persona o entidad una clave pública. Un certificado digital que siga el standard X509v3, utilizado por los navegadores, deberá contener la siguiente información:

1. Identificación del titular del certificado: Nombre, dirección, etc.
2. Clave pública del titular del certificado.
3. Fecha de validez.
4. Número de serie.
5. Identificación del emisor del certificado.

Asimismo las autoridades de Certificación pueden emitir diferentes tipos de certificados:

Los certificados de Identidad: ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.

Los certificados de Autorización o potestad: aquellos que certifican otro tipo de atributos del usuario distintos a la identidad.

Los Certificados Transaccionales: aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero.

Los Certificados de Tiempo o estampillado digital de tiempo: permiten dar fe de que un documento existía en un instante determinado de tiempo.

La Comisión Europea distingue las Autoridades de certificación (AC), cuyo objetivo esencial es "autenticar la propiedad y las características de una clave pública, de manera que resulte digna de confianza, y expedir certificados".

Funciones de las Autoridades de Certificación.

Algunas de las funciones de una Autoridad de Certificación según José Cuervo[107] son:

1. Generación y Registro de claves.
2. Identificación de Peticionarios de Certificados.
3. Emisión de certificado.
4. Almacenamiento en la AC de su clave privada.
5. Mantenimiento de las claves vigentes y revocadas.
6. Servicios de directorio.

Autoridades Públicas de Certificación.

Las autoridades de certificación (public key infrastructure" prevén generalmente una estructura jerarquizada a dos niveles: El

[107] José Cuervo, http://www.informatica-juridica.com/trabajos/firma_digital.asp

nivel superior suele estar ocupado por las autoridades públicas, que es la que certifica a la autoridad subordinada, normalmente privada.

a.2- LOS PRESTADORES DE SERVICIOS.

Los Prestadores de Servicios de Certificación son "las personas físicas o jurídicas que expidan certificados al público, y también las que además presten otros servicios relacionados con la firma electrónica (como los de consignación de fecha y hora, los de directorio o archivo de documentos electrónicos), por lo tanto, certifican la identidad de quien firma el documento electrónico que utiliza las claves de quien dice ser."[108]

Estos Prestadores responderán civilmente por daños y perjuicios que causen a sus usuarios o a terceros cuando actúen con negligencia en el incumplimiento de sus obligaciones.

Las obligaciones de estos Prestadores, certificación son[109]:

1. Comprobar la identidad y circunstancias de los solicitantes.

[108] AGM – LAWROPE- Abogados. http://www.efranquizium.com/articulos/nuevas_tecnologias/agm.asp

[109] AGM – LAWROPE- Abogados. http://www.efranquizium.com/articulos/nuevas_tecnologias/agm.asp

2. Dar al signatario el dispositivo de creación y verificación de firma.
3. No almacenar ni copiar datos de creación de firma del solicitante.
4. Informar de precio, condiciones de uso y limitaciones del Certificado.
5. Mantener un registro de certificados emitidos.
6. Si cesan en la actividad, comunicarlo varios meses antes a los titulares de los certificados.
7. Inscritos en el Registro de Prestadores de Servicios de Certificación.
8. Indicar la fecha y hora de expedición cuando corresponda.
9. Demostrar fiabilidad en sus servicios.
10. Garantizar la rapidez y seguridad en la prestación del servicio.
11. Adoptar medidas contra la falsificación de certificados.
12. Disponer de recursos económicos suficientes para afrontar el riesgo de su responsabilidad por daños y perjuicios.
13. Utilizar sistemas fiables para almacenar certificados.

a.3- EL REGISTRO O REPOSITORY (EN INGLÉS)

"Son la base de datos a la que el público puede acceder en línea (on-line) para conocer la validez de los certificados, su vigencia o cualquier otra circunstancia que se relacione con los mismos."[110]

La base de datos deberá incluir entre otros aspectos:

1. Los certificados publicados en el registro.
2. Las notificaciones de los certificados vencidos, suspendidos y revocados.
3. Las Autoridades Certificantes autorizadas.

Un dato importante es que para que el registro sea reconocido deberá estar bajo la tutela de un prestador de servicios o una autoridad certificante, esto con el fin de evitar obstáculos y proporcionar mayor seguridad.

a.4- SIGNATARIO.

"…Persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa."[111]

---

[110] Fernando Ramos Suárez, COMO APLICAR LA NUEVA NORMATIVA SOBRE LA FIRMA ELECTRÓNICA, febrero 2000, www.lagalia.com

[111] El caso de la Compra Venta en línea o Internet, San José; tesis de Licenciatura en Derecho, Universidad de Costa Rica, Pág. 285, 1997.

Este es el emisor del mensaje que se desea enviar a "X" o "Y", de manera que exista un respaldo jurídico y una seguridad de que dicho documento fue enviado por el mismo.

Es así como "…toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria…"[112].

a.5- RECEPTOR.

Es la persona a quien recibe el mensaje, comúnmente es a quien va dirigido el mensaje de datos, con el cual se cumple la finalidad de todo el proceso de certificación y/o envío por medio de la firma digital.

El objetivo de utilizar la firma digital es "acreditar quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad)"[113].

Impidiendo de esta forma que después se pueda "…negar su autoría (no revocación). De esta forma el autor queda vinculado al

[112] Ley Modelo sobre Comercio Electrónico, artículo 9 inciso 2, 1996.

[113] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 97.

documento que firma. Cualquier persona puede verificar la validez de una firma si dispone de la clave pública del autor."[114]

Con todo lo anterior observamos que la firma digital cumple todos los elementos formales necesarios, para la aplicación del negocio jurídico como tal.

b.- ELEMENTOS MATERIALES O DE FONDO.

Para empezar se necesita una computadora, una conexión a Internet sin importar cuál sea, una dirección de Internet segura **https** que son las "Direcciones de Internet seguras cuando Vd (direcciones virtuales) accede a una web con este encabezado el navegador le informará con una llave o un candado cerrado en la parte izquierda (si usa Netscape) o un candado cerrado en la parte derecha (si utiliza Explorer). Este hecho indica que nos estamos comunicando con un Web que tiene un certificado."[115]

A pesar de que al utilizar la firma digital no se quiere limitar a una sola tecnología o avance, es indispensable para su utilización, poseer

---

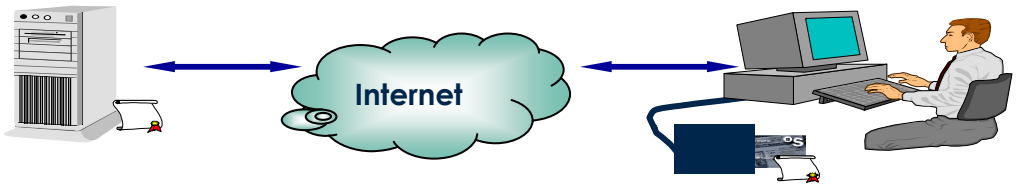
[114] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 98.

[115] Anónimo, Preguntas y respuestas, http://www.senacyt.gob.pa/firmadigital/preguntasrespuestasiv.htm

un ordenador con Procesador Pentium y por lo menos ocho Megabytes de RAM.

En relación con el software que necesito para instalar un certificado, este deberá ser un navegador obligatoriamente, Netscape Communicator o Microsoft Internet Explorer en sus versiones 4.0 o superiores. En relación a Windows 95, 98 o NT.

Además, si se trata de un certificado SET (Secure Electronic Transaction o en español Transacciones Electrónicas Seguras), necesitará una aplicación específica denominada Wallet (cartera electrónica) para gestionarlos.



c.- ELEMENTOS FUNCIONALES.

En relación con la firma podemos distinguir una doble función:

Identificadora

Asegura la relación jurídica entre el acto firmado y la persona ya sea física o jurídica que lo ha firmado.

La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones.

Asimismo, la firma digital nos expresa la identidad, aceptación y autoría del firmante.

Autenticadora

El autor del acto expresa su consentimiento y hace propio el mensaje. A su vez "permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, bien para garantizar el acceso a servicios distribuidos en red. En este último caso, la utilización de firmas digitales para acceder a servicios de red o autenticarse ante servidores web evita ataques comunes de captación de contraseñas mediante el uso de analizadores de protocolos (sniffers) o la ejecución de reventadores de contraseñas."[116]

d.- REQUISITOS DE LA FIRMA DIGITAL.

Según el Real Decreto-Ley 14/1999, de 17 de setiembre, la firma deberá estar

- Basada en un certificado reconocido que es un certificado que contiene la información descrita en su artículo 8 del RDL, (a.-

[116] Hugo Daniel Carrion, http://www.informatica-juridica.com/trabajos/analisis_comparativo_a_nivel_mundial_sobre_firma_digital.asp

Indicación de que se expiden como tales, b.- Código identificativo único del certificado, c.- Identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral, d.- La firma digital avanzada o digital del prestador de servicios de certificación que expide el certificado, e.- La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, siempre que aquel de su consentimiento, f.-En los supuestos de representación, la indicación del documento que acredita las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente, g.-Los datos de verificación de firma que correspondan a los datos de creación de la firma que se encuentra bajo el control del signatario, h.- El comienzo y el fin del período de validez del certificado, i.- Los límites del uso del certificado y j.- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen) y es

expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en artículo 12 del RLG.

- Creada por un Dispositivo seguro de creación de firmas el cual deberá contener los requisitos del artículo 19 del RDL (1. Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto, 2. Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento, 3. Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros, 4. Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.)
- Certificado expedido por Prestador de Servicios acreditado, se encuentra estipulado en el artículo 6 del RDL (1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que

permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios, 2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en la Ley 21/1992, de 16 de julio, de Industria y en la demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1, establecerá las condiciones que permitan coordinar los sistemas de certificación, 3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen, 4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior, valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que se haya pedido

certificación. También tomarán en cuenta el cumplimiento por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado, 5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

- El Dispositivo seguro de creación de firma con el que ésta se produzca se encuentra estipulado en el artículo 21 del RDL (Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica: 1. Los órganos de certificación a los que se refiere el artículo 6, podrán certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de evaluación acreditadas. En la evaluación del cumplimiento de los requisitos previstos en el artículo 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el artículo anterior u otras que determinen los

órganos de acreditación y de certificación y cuyas referencias se publiquen en el "Boletín Oficial del Estado". 2. Se reconocerá eficacia a los certificados sobre dispositivos seguros de creación de firma que hayan sido expedidos por los organismos designados para ello por los Estados miembros de la Unión Europea, cuando pongan de manifiesto que dichos dispositivos cumplen los requisitos contenidos en la normativa comunitaria sobre firma electrónica.)

SECCIÓN SEGUNDA: UTILIZACION DE LA FIRMA DIGITAL.

a.- COMO INSTRUMENTO JURÍDICO.

La firma digital "tiene en relación con documento electrónico el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel. Por ello es obligatorio su admisión como prueba en juicio, la cual debe ser valorada conforme a los criterios de apreciación judicial establecidos en las normas procesales."[117]

Es decir que el firmante se encuentra acreditado y el dispositivo de creación de la firma empleado por el firmante esta certificado oficialmente, este no puede negar su autoría.

---

[117] Anónimo, Guía Sobre el Uso y Eficacia de la Firma Electrónica, http://www.mju.es/guia_f_elect.htm

"La firma acredita la autoría del documento subscrito normalmente al pie del mismo y representa la formalización del consentimiento y la aceptación de lo expuesto, y es por tanto origen de derechos y obligaciones.

La firma será válida siempre que no sea falsificada o se haya obtenido con engaño, coacciones o de cualquier otro ilícito proceder."[118]

No obstante algunas legislaciones imponen requisitos de escrito y de firma manuscrita como condición de validez o como condición de pruebas de ciertos contratos y actos jurídicos. Por lo tanto, para que desde un punto de vista legal estos contratos sean reconocidos, la jurisprudencia deberá interpretar el término firma y escrito de forma suficientemente amplia para acoger la firma digital, o bien debe modificarse la ley tratando de asimilar la firma digital a la firma manuscrita.

En Costa Rica, no se ha probado la validez legal de la firma digital ante los tribunales de justicia, no existiendo por ello las garantías jurídicas plenas para su uso. Sin embargo, por el entorno criptográfico

[118] José Cuervo, La Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

"se considera la firma digital con capacidad superior a la manuscrita, ya que no sólo comporta la autenticidad del documento firmado, sino su integridad; o lo que es lo mismo, la certidumbre de que no ha sido alterado en ninguna de sus partes."[119]

El borrador de directiva comunitaria, realiza un reconocimiento de los efectos de la misma, equiparándola, con más o menos exigencias, a la firma manuscrita. Estableciéndose en su artículo 5.2 que los Estados miembros asegurarán que las **firmas digitales**[120] basadas en certificados cualificados emitidos por un proveedor de servicios de certificación, que cumpla los requisitos establecidos en el anexo II:

a) satisfacen las exigencias legales de firma manuscrita

b) son admisibles como medio de prueba en procedimientos legales de la misma forma que las firmas manuscritas.

En relación con todo lo anterior tenemos que tener presente las principales directrices que busca la firma digital "la libre

[119] José Cuervo, La Firma Digital y Entidades de Certificación, http://www.informatica-juridica.com/trabajos/firma_digital.asp

[120] El término firmas digitales y la negrita no corresponde al texto original, debido a que en este se estipula firmas electrónicas, dicho término ha sido modificado para evitar confusiones en cuanto al tema de investigación, es importante reafirmar como bien lo estipula: J. Andrés Hall y Mauricio Devoto, en su libro La Firma Digital: Herramienta Habilitante del Comercio Electrónico, Pág. 27 "…corresponde hablar de firma digital y no de firma electrónica, vocablo este último que se utiliza erróneamente en cierta legislación internacional para referirse a la firma mecanizada para los fines de su procesamiento informático, la que consiste más precisamente de dígitos (binarios) que de electrones.

competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia de la firma digital a la firma manuscrita.

1. Promover la compatibilidad con el marco jurídico internacional. Este principio refiere a la dimensión global o internacional del tema desde el punto de vista legislativo y tecnológico, a fin de permitir la inserción en el mercado mundial del comercio electrónico.

2. Asegurar la neutralidad tecnológica: Se hace referencia aquí a la no discriminación entre distintas tecnologías y, en consecuencia la necesidad de producir normas que regulen los diversos entornos tecnológicos. Este principio refiere a la flexibilidad que deben tener las normas, es decir, que las mismas no estén condicionadas a un formato, una tecnología, un lenguaje o un medio de transmisión específico.

3. Establecer la equivalencia de la firma digital a la firma manuscrita, considerando que la misma satisface el requerimiento de firma respecto de los datos consignados en forma electrónica y tiene los mismos efectos jurídicos que la firma manuscrita con relación a los datos consignados en papel.

4. Establecer la libre competencia con respecto a todos los servicios relacionados con la certificación de las firmas electrónicas."[121]

De conformidad con la Ley Modelo de la CNUDMI sobre Comercio Electrónico, 1996, podemos ir analizando algunos artículos importantísimos referentes a la firma digital, entre los más destacados respecto al tema que se esta desarrollando son los siguientes:

Artículo 5, expresamente nos habla del reconocimiento jurídico, brindándole a su vez validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensajes de datos, enunciando de esta forma el principio fundamental de no discriminación, considerándose que no puede existir disparidad alguna respecto con los documentos consignados sobre papel.

Este es un principio de aplicación general, por lo que no debe limitarse en su alcance, y mucho menos denegar su eficacia jurídica, validez o fuerza ejecutoria por la forma en que se haya conservado la información.

[121] Conclusiones Generales de la Comisión De Firma Digital, Dra. Gabriela Guerriero, Dr. Mario Maio, Dra. Marina Mongiardino, Dr. Diego Rull, Dra. Carolina Vega, Dra. Mercedes Velásquez, http://www.aadat.org/conclusiones_generales42.htm

Artículo 7, en este se destacan las funciones de la firma, las cuales tenemos que mantener en consideración tales como: identificar a una persona, dar certeza a la participación personal de esa persona en el acto de firmar, y asociar a esa persona con el contenido de un documento.

De las anteriores se desprenden otras más según la naturaleza del documento firmado. Por ejemplo intención de una parte contractual de obligarse con el contenido del contrato firmado, el hecho de que el firmante se encontraba en un lugar determinado, el hecho de que el firmante se encontraba en el momento dado, etc.

No obstante para la aceptación de dichas funciones deberá realizarse con ciertas indicaciones y métodos para que obstente validez el mensaje.

Artículo 9, el cual es uno de los más importantes debido a que es en este que se estipula el reconocimiento de admisibilidad y fuerza probatoria, por lo que toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria, teniendo siempre presente la fiabilidad de la forma en que se haya generado, archivado o comunicado el mensaje así como su conservación e integridad de la información.

De esta forma se logra establecer "la admisibilidad de los mensajes de datos como pruebas en actuaciones legales y su fuerza probatoria,… por lo que no debe negarse la admisibilidad de los mensajes de datos como pruebas en actuaciones judiciales por la sola razón de que figuran en formato electrónico."[122]

Artículo 11, el cual crea validez o fuerza obligatoria de un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.

"Se promueve el comercio internacional dando mayor certeza jurídica a la celebración de contratos por medios electrónicos. El artículo no trata solamente de la formación del contrato sino también de la forma en que cabría expresar la oferta y la aceptación de la misma."[123]

Artículo 12, Reconoce entre las partes los mensajes de datos, al cual no se le negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración.

"La formación de un contrato no es sino uno de los supuestos ilustrativos que pueden ser valiosos a este respecto, por lo que se juzgó

[122] Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para la Incorporación al Derecho Interno 1996, Naciones Unidas Nueva York, 1997, Pág.43,44.
[123] Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para la Incorporación al Derecho Interno 1996, Naciones Unidas Nueva York, 1997, Pág. 45, 46.

necesario ilustrar también la validez jurídica de expresiones unilaterales de la voluntad, tales como notificaciones o declaraciones unilaterales de voluntad emitidas en forma de mensaje de datos."[124]

La Ley Modelo permite "a los Estados adaptar su legislación en función de los avances técnicos de las comunicaciones aplicables al derecho mercantil, sin necesidad de eliminar por completo el requisito de un escrito ni de trastocar los conceptos y planteamientos jurídicos en que se basa dicho requisitos."[125]

Asimismo, la Ley Modelo "sigue un criterio denominado "criterio de equivalencia funcional", basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico."[126]

La documentación consignada por medios electrónicos puede ofrecer una seguridad equivalente al documento de papel, y hasta

[124] Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para la Incorporación al Derecho Interno 1996, Naciones Unidas Nueva York, 1997, Pág. 47, 48.
[125] Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para la Incorporación al Derecho Interno 1996, Naciones Unidas Nueva York, 1997, Pág.19.

[126] Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para la Incorporación al Derecho Interno 1996, Naciones Unidas Nueva York, 1997, Pág. 21.

puede ofrecer mayor fiabilidad y rapidez, en la determinación del origen y contenido de los datos.

Entre las funciones que cumple el documento de papel y que a su vez se cumplen en el documento electrónico tenemos:

1. Proporcionar un documento legible para todos.
2. Asegurar la inalterabilidad de un documento a lo largo del tiempo.
3. Permitir la reproducción a fin de que cada una de las partes disponga de un ejemplar del mismo escrito.
4. Permitir la autenticación de los datos consignados.
5. Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales.

b.- MÉTODO PARA APLICAR LA FIRMA DIGITAL.

A lo largo de esta investigación deben estarse preguntando ¿Cómo se usa la firma digital?, esta a pesar de parecer muy complicada en realidad es muy simple, por lo que se procederá a detallarse de la siguiente forma:

1. Se debe contar con un ordenador con conexión con Internet y con un dispositivo lector de tarjetas de firma digital.

2. Debemos acudir a un Prestador de Servicios de certificación, que procederá a nuestra identificación personal.
3. Este Prestador de Servicios generará dos claves, una pública y otra privada.
4. El Prestador de Servicios nos entregará la tarjeta o el disquete que contenga esta clave privada, así como el programa necesario para su uso, y
5. Se debe instalar dicho programa en nuestro ordenador.

Con todo lo anterior se estaría listo para la firma de un documento o archivo que se haya creado, el cual además podemos encriptar y enviarlo vía correo electrónico a quien deseemos, junto con el certificado de nuestro Prestador de Servicios que confirma nuestra identidad.

No obstante, la firma digital se realiza de la siguiente forma:

"El software del firmante aplica de forma transparente al usuario un algoritmo hash sobre el texto a firmar, obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje (un mínimo

cambio en el mensaje produce un extracto completamente diferente). Los algoritmos hash más utilizados son MD5 ó SHA-1."[127]

"Este extracto, cuya longitud oscila entre 128 y 160 bits (en función del algoritmo utilizado), se somete a continuación a cifrado mediante la clave secreta del autor, previa petición de contraseña. El algoritmo utilizado para cifrar el extracto puede ser el mismo RSA o una clave específica para firmar tipo DDS. El extracto cifrado constituye la firma y se añade la final del mensaje (o en un archivo adherido a él)."[128]

Para comprobar la validez de la firma digital se necesitará disponer de la clave pública del firmante para poder corroborar los datos, así como si estos se encuentran vigentes.

Después de aplicarle la clave pública el software del receptor descifra el extracto cifrado que constituye la firma digital y como resultado se obtiene un bloque de caracteres.

Se calcula el extracto hash que corresponde al texto del mensaje y si el resultado coincide exactamente con el bloque de

---

[127] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 98.

[128] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 98.

caracteres en la primera operación, la firma se considera válida, debido a que de existir la menor diferencia, la firma se considera como no valida.

La firma logra comprobar por si sola la relación entre el mensaje y la clave utilizada, pero para asegurar que esa clave corresponde a quién dice poseerla es que necesitamos de la intervención de una tercera parte confiable, en la que ambas partes interesadas confíen; estas partes son las que comúnmente se denominan Autoridades de Certificación.

Algunos programas no utilizan esta última, debido a que delegan en el usuario la responsabilidad de certificar claves conforme con su criterio, estas comúnmente se llaman redes de confianza o en inglés Web of trust, totalmente descentralizada, pero con el apoyo de una red de servidores de claves como "The Global Trust register", el cual es un directorio que contiene las principales claves públicas del mundo, verificando de esta forma la validez de los certificados X.509 y algunas claves públicas.

"… Verisign y Thawte son las autoridades de certificación más reconocidas a nivel mundial."[129]

En resumen el método por utilizar es el siguiente:

"Cada persona obtiene un par de claves llamadas clave pública y clave privada. Cada usuario debe generar su propio par de claves, por intermedio de un software confiable. La clave pública de cada persona la publica y la privada se mantiene en secreto. La necesidad de un remitente y un receptor de compartir la misma clave queda eliminada. Ya no es necesario confiar en los canales de comunicación, corriendo el riesgo de que alguien esté escuchando en la línea telefónica o de que se viole el secreto de la clave privada. Cualquier persona puede enviar un mensaje confidencial con sólo utilizar la clave pública, pues el mensaje solamente puede desencriptarse con la clave privada que posee el receptor únicamente."[130]

A la hora de enviar un certificado los usuarios comúnmente utilizan los navegadores Netscape o Explorer, sin embargo ambos

---

[129] Victoria del Rosario Pivaral Leal y Giovanni Obdulio Cajón Arrianza, Tesis: "Comercio Electrónico en Internet: E-Comerce", Universidad Francisco Marroquín, Facultad de Ingeniería de Sistemas, Informática y Ciencias de la Computación, Guatemala 2000. Pág. 100.

[130] Guía sobre el Uso y Eficacia de la Firma Electrónica, http://www.mju.es/guia_f_elect.htm

requieren un proceso diferente para enviarlos o exportarlos a su destinatario el cual consiste en el siguiente:

De Netscape a Internet Explorer[131], los pasos que tiene que realizar son:

1. Abrir Netscape Correo.
2. Click en seguridad
3. Ver certificados personales.
4. Elegir el certificado a exportar.
5. Click en Exportar.
6. Darle un nombre, unidad y ruta.
7. Aceptar.
8. Abrir Explorer.
9. Menú Ver.
10. Seleccionar opciones de Internet.
11. Seleccionar contenido.
12. Seleccionar certificados: personal.
13. Importar.
14. Mensaje importar certificados. Deberá seleccionar qué

[131] Si se desea profundizar más en los pasos a seguir se puede visitae le sitio Web "Preguntas y Respuestas", http://www.senacyt.gob.pa/firmadigital/preguntasrespuestasiv.htm

certificados utilizará. Incluir la contraseña con la que protegió la exportación del certificado. Incluir el nombre y la localización (ruta o path) del certificado a importar.

15. Pulsar aceptar.

De Internet Explorer a Netscape, [132]los pasos que tiene que realizar son los siguientes:

1. Abrir Explorer.

2. Menú Ver.

3. Seleccionar opciones de Internet.

4. Seleccionar contenido.

5. Seleccionar certificados: personal.

6. Exportar.

7. Mensaje exportar certificados. Deberá seleccionar qué certificado utilizará. Incluir el nombre y la localización (unidad de diskette) del certificado por exportar.

8. Abrir Netscape Correo.

9. Click en seguridad

10. Ver certificados personales.

11. Seleccionar el botón importar.

[132] Si se desea profundizar más en los pasos a seguir se puede visitae le sitio Web "Preguntas y Respuestas", http://www.senacyt.gob.pa/firmadigital/preguntasrespuestasiv.htm

12. Seleccione un nombre, unidad y/o ruta desde la que va a importar (normalmente unidad A:).

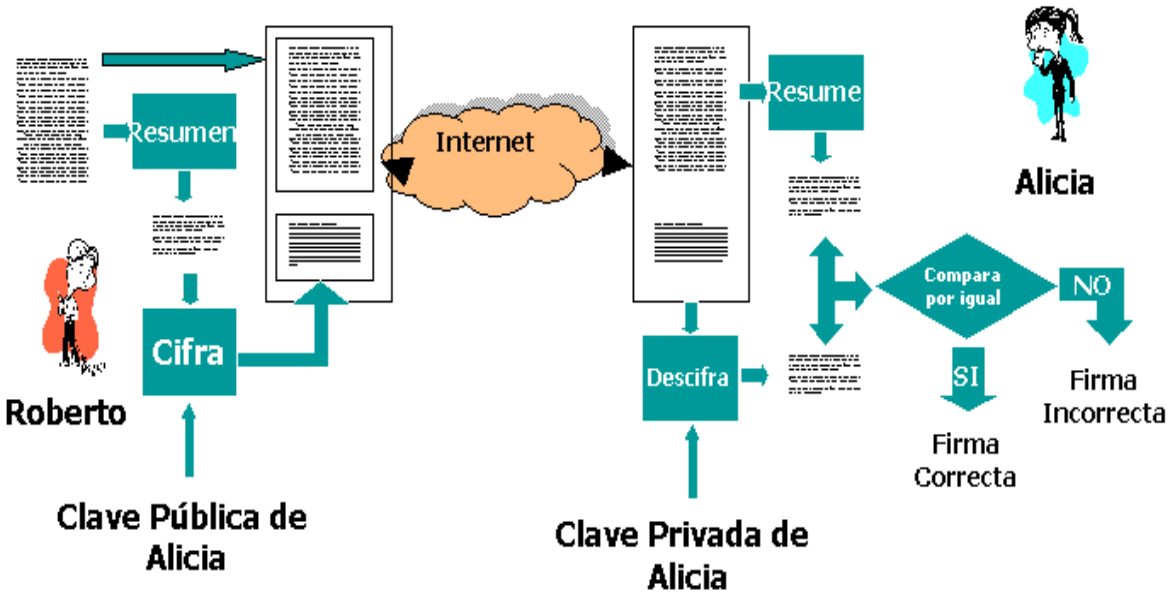
13. Se le solicitará la contraseña con la protegió la exportación de su certificado.

14. Aceptar.

Es importante señalar que se pueden firmar por este medio todo tipo de documentos que no estén sujetos a exigencias determinadas.

El siguiente es un gráfico que explica el proceso de aplicación de la firma digital:

Proceso de Firma Digital.[133]



[133] Anónimo, Guía Temática, http://www.diputados.gov.ar/guia_tematica.html

En el gráfico anterior podemos ver como Roberto desea enviarle un mensaje a Alicia, así que confecciona el mensaje, Roberto le agrega la clave pública de Alicia la cual se encuentra en un registro "X" con esta clave cifra o codifica el documento que es enviado a Alicia vía correo electrónico utilizando Internet.

Alicia recibe el mensaje que esperaba de Roberto le agrega su clave privada de la cual sólo ella tiene conocimiento, el documento es comparado inmediatamente y si coincide con la numeración dada por el algoritmo, Alicia lo acepta y adquiere validez.

Pero si el mensaje no coincide con la numeración dada por el algoritmo, es por que fue alterado en el camino a su destino, por lo que el mensaje sería inválido.

CAPÍTULO SEGUNDO.

TRANSACCIONES COMERCIALES EN INTERNET UTILIZANDO LA FIRMA DIGITAL.

SECCIÓN PRIMERA: VENTAJAS Y DESVENTAJAS AL REALIZAR TRANSACCIONES COMERCIALES, UTILIZANDO LA FIRMA DIGITAL.

a.- VENTAJAS.

La firma digital acarrea múltiples ventajas y beneficios, no obstante el sector servicios es el que recibirá mayores beneficios con la promulgación de una ley. Muchos de los servicios que se realizan hoy en día a través de Internet son: "EDI, servicios financieros, negocios B2C (multitiendas), B2G, B2B (compra de insumos de una empresa a otra), mensajería electrónica secreta, traspasos de fondo ultra seguros hechos por los propios poseedores de cuentas bancarias, trabajo cooperativo, educación a distancia, servicios de la administración pública como los trámites y el pago de impuestos. Adicionalmente, la promulgación de la ley ayudará a consolidar a ciertos servicios que ya se prestaban en la red, pero de manera muy precaria, como los servicios de laboratorio, arquitectura, ingeniería,

contabilidad y legales, los cuales para su total ejecución a distancia requieren de firma electrónica con vigencia legal para tener validez."[134]

No obstante la sola promulgación de la ley, no significaría la implementación en los procesos y documentos judiciales debido a que los mismos necesitarán de una mecánica judicial diferente que garantice su buen funcionamiento.

Debido a la naturaleza de la firma digital es que esta puede ser realizada en diferentes puntos del mundo de manera simultánea y sin necesidad de testigos, siendo compatible está con los dispositivos electrónicos actuales, ya que los programas pueden estar almacenados en cualquier procesador contenido en un Smart Card, en una Note Book, en una PC, etc.

Algunas de las ventajas generales que nos ofrece la firma digital son las siguientes:

- Proporciona el máximo grado de confidencialidad y seguridad en Internet.

[134]Paola Passig V, Firma electrónica, Adiós Papel, 7 de abril de 2002, http://www.mercuriovalpo.cl/site/apg/reportajes/pags/20020406235922.html

- Identifica a las partes que se conectan.
- Da acceso a una inmejorable oferta de servicios en el ámbito de la gestión de los derechos de autor.
- Declaración de la Renta o la del IVA.
- Permite hacer más eficientes las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
- Reduce las barreras de acceso a los mercados actuales.
- Reduce o incluso elimina por completo los intermediarios.
- Brinda información rápida y precisa en el lugar indicado.
- Permite un mejor planeamiento de la recepción y el despacho de mensajes.
- Seguridad en el procesamiento de transacciones, se eliminan los errores por el reingreso de información.
- Reducción de costos administrativos.
- Disminuye notablemente la cantidad de documentos impresos.
- Comunicación permanente las 24 horas los 365 días del año.

No podemos dejar de lado las ventajas y aplicaciones que dicha figura brindaría dentro del marco jurídico tales como:

- **Autenticación:** "permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, bien para garantizar el acceso a servicios distribuidos en red."[135]Garantizando de esta forma que el mensaje ha sido realizado por la parte identificada en el documento como emisor.
- **"Imposibilidad de suplantación:** el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, control biométrico, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo."[136]Creando una seguridad casi indiscutible sobre la autoría del mensaje mismo.
- **Integridad:** "La integridad del documento es una protección contra la modificación de los datos en forma

[135] Anónimo, Firma Digital, 12 de enero de 2002, http://www.delitosinformaticos.com/ecommerce/contratos.shtml.

[136] Anónimo, Firma Digital, 12 de enero de 2002, http://www.delitosinformaticos.com/ecommerce/contratos.shtml

intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre le documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia."[137]

- **No repudio:** "ofrece seguridad inquebrantable de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma electrónica adjunta a los datos, debido a la imposibilidad de ser falsificada, testimonia que él, y solamente él, pudo haberlo firmado."[138]
- "**Auditabilidad:** permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la

[137] Blanch, Leonardo Cabrera, Federico M, Cafure, Martín J,Transmisión Segura de Documentación-Firma Digital, www.monografias.com.

[138] Anónimo, Firma Digital, 12 de enero de 2002, http://www.delitosinformaticos.com/ecommerce/contratos.shtml.

presentación de certificados, especialmente cuando se incorpora el estampillado de tiempo, que añade de forma totalmente fiable la fecha y hora a las acciones realizadas por el usuario."[139]

- **Acuerdo de claves secretas:** "garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no…"[140]realizando transacciones seguras dentro de las cuales tanto el emisor como el receptor conocen del envió de mensajes utilizando las claves secretas de cada uno de los usuarios.

En resumen, la firma digital posee muchas ventajas en diferentes áreas, las cuales son importantísimas para el desarrollo de un país, uno de los factores más destacados de la firma digital es la seguridad[141], debido a que abarca múltiples tipos de esta algunas de las más significativas son:

---

[139] Anónimo, Firma Digital, 12 de enero de 2002, http://www.delitosinformaticos.com/ecommerce/contratos.shtml.

[140]Anónimo, Firma Digital, 12 de enero de 2002, http://www.delitosinformaticos.com/ecommerce/contratos.shtml.

[141] Si se desea ampliar el tema de la seguridad que puede brindar la firma digital, se puede accesar la dirección http://www.informatica-juridica.com/trabajos/aspectos_tecnicos.asp, dentro de esta misma se realizan trabajos con el fin de analizar diferentes aspectos técnicos y prácticos sobre la figura que se ha ido desarrollando a lo largo de esta investigación.

1. **Seguridad Técnica**, permite obtener comunicaciones privadas, auténticas e íntegras entre las partes evitando que los piratas informáticos o "hackers" invadan las mismas.
2. **Seguridad Jurídica**, regula el marco jurídico de las posibles conductas o actos ilícitos que se puedan realizar utilizando Internet, creando a su vez responsabilidades por los acto realizados.
3. **Seguridad mercantil o económica**, utilizando la seguridad jurídica, logra asegurar y garantizar las transacciones financieras, mercantiles o de intercambio comercial realizadas a través de la red.
4. **Seguridad a los consumidores**, garantiza a los consumidores la responsabilidad ante las actuaciones realizadas asimismo evita el abuso de empresas que acostumbran utilizar cláusulas abusivas.

Como bien lo estipula José Antonio Rodríguez Corrales, la firma digital será una "herramienta de competitividad, al permitir el liderazgo en la reducción de costos, la diferenciación de productos y la identificación de segmentos del mercado…"[142] convirtiéndose la misma en "un instrumento necesario e indispensable para el control en todas las áreas de la administración pública."

b.- DESVENTAJAS.

No obstante de todos los grandes beneficios que complementan la firma digital, existen algunas desventajas de la misma, sin embargo muchas de estas se deben a la falta de cultura y educación que es indispensable para la compresión, de una figura tan delicada y moderna como lo es la firma digital.

La más destacada desventaja que encontramos no sólo en Costa Rica sino en muchos países, es que a diferencia de la firma manuscrita la firma digital no es legalmente aceptada en muchos países, debido a la falta de legislación que garantice dicha figura, asimismo por ser una tecnología tan nueva genera temor y rechazo.

Por su naturaleza la firma digital posee dos claves una privada y una pública, dependiendo de la primera la seguridad y

[142] José Antonio Rodríguez Corrales, Director General de Aduanas, Asamblea Legislativa, Expediente 14276, folio 961

confidencialidad del mensaje, no obstante si esta es adquirida y usada por individuos no autorizados, se compromete la seguridad del mensaje de datos.

Otro punto importante es que al trabajar con tecnología nos hemos ido dando cuenta de que esta cambia constantemente, por lo que la firma digital al depender de la tecnología misma podría comprometer la validez e integridad del mensaje de datos que se llevo acabo utilizando la firma digital.

Don Edgar Delgado señala en su reportaje al periódico La Nación que "el principal obstáculo de nuestros países es la infraestructura de telecomunicaciones, la cual obstaculiza el comercio electrónico en dos vías: a través del alto costo de las conexiones y la escasa penetración de los servicios en diversas áreas."[143]

Asimismo, señaló "que en este momento es necesario un proceso de "culturalización" de los empresarios, para que comprendan la importancia del comercio electrónico."[144]

---

[143] Edgar Delgado M, Gran potencial en Internet, Abrirán certificadora de firmas digitales, La Nación 3 de diciembre de 2001.

[144] Edgar Delgado M, Gran potencial en Internet, Abrirán certificadora de firmas digitales, La Nación 3 de diciembre de 2001.

Algunos de los factores que afectan negativamente la firma digital son los siguientes:

- **Necesidad de Infraestructura de computadora e Internet:** como anteriormente lo mencionó Don Edgar Delgado, para utilizar la firma digital necesitamos de diferentes elementos entre ellos los más importantes son una computadora y una conexión a Internet, porque sin estos sería imposible llevar a cabo la firma digital, es así como la falta de alguno de estos dos elementos nos impide la utilización de los mismo. El problema radica en que no todo el mundo posee una computadora en su hogar o trabajo por lo que les impide la utilización de la firma digital.

- **Costos amplios para el gobierno, infraestructura y educación:** al buscar la participación del gobierno en la utilización de la firma digital, caemos en la fría y cruel verdad que abarca desde los costos hasta la educación. Los costos de implementar el equipo e infraestructura necesaria para desarrollar el uso de la firma son altos y de

existir presupuesto para la compra de los mismos, nos enfrentaríamos al obstáculo de educar y capacitar al personal, el cual puede que muchas veces ni siquiera haya utilizado Internet una vez en su vida, por lo que el entender el manejo y función de la firma puede ser muy complicado y de un costo muy amplio, debido a que la capacitación y educación empezaría desde conceptos muy elementales.

- **Temor e inseguridad en la utilización de la firma:** al pasar los años nuevas tecnologías han ido surgiendo y teniendo éxito, no obstante no existe una absoluta confianza de las partes que intervienen directamente al realizar una transacción electrónica, ejemplo de esto son las tarjetas de crédito, las cuales a pesar de que han demostrado su confiabilidad, muchas personas temen utilizarlas para realizar cualquier tipo de transacción en la cual se utilice Internet. Esto se debe a la gran cantidad de piratas o hackerds que han realizado múltiples fraudes utilizando las tarjetas de crédito.

- **Cultura de papel:** este es un aspecto muy difícil de corregir ya que se basa simplemente en la costumbre que maneja y enseña un determinado país a sus habitantes. Desgraciadamente Costa Rica no es la excepción a la regla, durante muchos años se ha manejado la cultura del papel en todas las áreas, prefiriendo la gente mantener todos sus títulos, certificados, números de cuenta, claves e incluso datos poco relevantes, como la fecha de cumpleaños de una amigo o el numero telefónico de este, de una manera mucho más tangible o material como lo es la escrita en soporte de papel.

- **Estándares de seguridad y de legislación:** la naturaleza de la firma digital permite el desarrollo de la misma en diversos medios, lugares y tiempos, sin embargo es importante que para el desarrollo de la firma digital contemos con un estándar mundial que facilite su regulación, de no ser así nos encontraríamos con problemas de legitimación y validez de los actos

realizados utilizando la firma digital, quedando desprotegida alguna de las partes intervienientes.

- **Tipificación de delitos cibernéticos:** a pesar de que la firma digital es considerada un medio seguro para realizar transacciones, como en toda figura existen excepciones a la regla, por lo que la falta de legislación en lo concerniente a delitos cibernéticos o informáticos constituye un obstáculo para la utilización segura, libre y confiable de la firma digital.

- **Administración compleja:** no es tan fácil como chasquear los dedos, la administración de la firma digital requiere de diversos análisis y estudios para poder determinar quién, quiénes, cómo, dónde y cuándo pueden participar en la utilización de la firma digital ya sea de una manera activa o pasiva.

- **Claves deberán ser guardadas de manera centralizada:** no podemos tener nuestras claves que autorizan la

utilización de la firma digital regadas en cualquier parte, porque de ser así cualquier persona podría utilizar las mismas haciéndose pasar por uno de nosotros, vinculándonos con obligaciones y responsabilidades que talvez no deseamos. No obstante se debe tener cuidado al manejar este aspecto, ya que al decir centralizada no se debe entender que favorece la creación de monopolios o grupos similares al respecto.

- **No permite el no repudio:** esta figura por la seguridad que alcanza, no acepta el rechazo de una actuación o transacción realizada con las claves correctas de un determinado sujeto, esto se debe a que las claves corresponden a un individuo en particular el cual debe velar por el debido cuidado y custodia de las mismas. Lo cual en el caso de estar coaccionado por alguien o algo en un determinado momento, el sujeto no puede negar su autoría y deberá responder por su actuación.

- **Pérdida de la unidad del acto:** la unidad del acto es un elemento que a pesar de que se encuentre debidamente estipulado en el Código Notarial, se ha venido perdiendo y tergiversando, en cuanto cada día son más los asistentes de abogados que recogen firmas en distintos momentos y lugares. Con la utilización de la firma digital podríamos asegurar que prácticamente este elemento desaparece, para asegurar otros elementos como la autenticidad, la integridad y la fiabilidad.

- **Precios de la tarifas de cada país:** La firma digital facilita y evita en múltiples ocasiones el traslado a un país para la firma y acuerdo de un determinado acto. No obstante como ya antes se había mencionado para la realización de la firma se necesita del Internet como elemento básico, sin embargo el precio del uso de este varía muchísimo de un lugar a otro y de la tecnología que se utilice, lo cual puede que acrecenté los costos para una parte más que a la otra, creando desigualdades al realizar las transacciones electrónicas.

SECCIÓN SEGUNDA: DIFERENTES TRANSACCIONES COMERCIALES QUE SE PUEDEN REALIZAR UTILIZANDO LA FIRMA DIGITAL.

Como podemos observar con el transcurso de esta investigación la firma digital posee múltiples ventajas y usos, "sirve para la identificación indubitable de una persona que emite un mensaje, transacción o documento en medios electrónicos. Es en definitiva, según la finalidad particular, el pasaporte, la llave del vehículo, la casa, la oficina, la identificación de autoría de un documento, un plano, una investigación científica, un software, el carnet de un club, y tantas otras aplicaciones como se pueda imaginar, con el importante incremento de la impersonalización que se produce día a día, imaginándonos que ciertas actividades se han realizado durante años por la simple emisión verbal y hoy requieren de un respaldo mayor, adicionándole la facilidad de ahorros importantes en el tiempo, costos y exactitud en la transmisión."[145]

Según las "Directrices del Memorándum de Acuerdo sobre libre acceso de las PYMEs europeas al comercio electrónico"[146] existen

[145] Lic. Daniel Edgardo Cortés, QUE ES LA FIRMA DIGITAL Y EL DOCUMENTO ELECTRONICO, http://www.fundaciondike.org/seguridad/firmadigital.html

[146] Estudio de situación del comercio electrónico en España, http://www.internautas.org/documentos/pista.htm, Esta tabla forma parte otro resultado del piloto Mercado Global para PYMEs es una guía de comercio electrónico para PYMEs [56], que trata diversos temas.

diversos tipos de transacciones comerciales que se pueden realizar, muchas de las cuales utilizan la firma digital de las cuales hablaremos más adelante.

No obstante según Rodolfo Lomascolo[147] los servicios y aplicaciones de la firma digital[148] se clasifican de la siguiente forma:

a.-Intercambio Electrónico de Datos (EDI):

Por medio del intercambio electrónico de datos, las empresas intercambian datos comerciales normalizados, tales como ordenes de compra, facturas, conocimientos, publicidad, cotizaciones, resúmenes de cuenta, recibos de pago, invitaciones, promociones, etc.

Imagínese la cantidad de dinero y tiempo, que podemos ahorrar utilizando este sistema, por ejemplo: en lugar de una boutique tenga que llamar a todos sus clientes y comunicarles que el día de mañana va a realizarse una promoción y que desean invitarlos al evento, les envían un mensaje de datos completamente personalizado, donde les asegure que solo sus clientes o las personas a las que se les está enviando dicha invitación recibirán la misma. Sus

[147] Rodolfo Lomascolo, Servicios y Aplicaciones de la Firma Electrónica, **r.lomascolo@mail.ips.es**, **www.ipsCA.com**

[148] Lo subrayado no corresponde al texto original, el mismo se ha modificado para efectos de la presente investigación y para evitar futuras confusiones, ya que el término firma es usado incorrectamente como firma electrónica por el señor Rodolfo, según las investigaciones realizadas.

clientes van a sentir un mejor trato personal y usted como dueño de la boutique va a poder confirmar que el mensaje sea recibido y a su vez cuanta gente va asistir al evento.

Otro ejemplo de esto son las órdenes de compra ya no tendrá que esperar un año a que llegue la pieza de su carro que tanto necesita, solo contacta con un distribuidor y puede realizar su orden de compra directamente evitándose todo tipo de intermediarios, problemas por la falta de su repuesto y estafas en la realización de sus pedidos, teniendo mucha más seguridad al realizar cualquier tipo de transacción.

En general se puede realizar el intercambio de datos en todas las áreas que las personas requieran. No obstante al utilizar la firma digital no aseguramos de que estos datos sean confidenciales, auténticos, íntegros y no repudiados.

b.- Servicios Financieros:

"La globalización del entorno financiero conlleva la posibilidad de poder contratar con una entidad situada en cualquier país. Esto permite a los consumidores elegir el producto o servicio que más convenga a sus intereses a unos precios más competitivos."[149]

[149] Estados Unidos Apuesta por el Comercio Electrónico, 4 de julio del 2000, Mercedes Asorev, http://www.expansiondirecto.com/2000/07/04/tecnologia/4tec.html

Lo que se busca establecer con estos servicios es crear "…canales directos, crear nuevos conceptos de valor, extender las fronteras, se incorporan las cadenas de valor, se desarrolla una nueva cultura, se genera mayor tráfico de transacciones y se crean programas de afiliación. Con estas premisas, las instituciones buscan mantener sus clientes fieles, quienes se identifican con su banco o su empresa de servicios financieros, basados en la confianza y credibilidad."[150]

Algunos de los servicios financieros más comunes son: los resúmenes de cuenta, recibos de pago, factura electrónica, cheque electrónico, tarjetas de crédito y prestación de servicios financieros en general.

c.- Negocios:

Debemos entender como negocio toda actividad que presente algún interés, utilidad e importancia tanto para las partes como el derecho en general siendo siempre su finalidad lucrativa o interesada.

"Los contratos a distancia hacen realidad el Mercado Único para las empresas y los consumidores, otorgándoles mayores

[150] Rodolfo Gasparri, Internet Banking será el Canal de Distribución por Excelencia, Abril/Mayo 2000, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

posibilidades de realizar negocios transfronterizos. Pero la disparidad normativa que actualmente existe en los países de la Comunidad puede impedir que los consumidores y empresarios se beneficien de la libre circulación."[151] A consecuencia de esto es que se desarrollan nuevas formas que se apliquen a las necesidades reales de los individuos.

Es así como vemos que los "negocios han obligado a redefinir al Banco y sus servicios, a estar más atentos a las nuevas realidades y a que los funcionarios reconozcan la importancia de su papel en este proceso de transformación."[152]

Debido a que es una forma de generar ingresos mucho más rápida y eficaz, además de ser parte de la nueva forma de hacer negocios; casi podríamos repetir las palabras del señor Presidente de los Estados Unidos de América, Bill Clinton quien dijo en un mensaje al Congreso que "…considera a Internet como la segunda revolución industrial. La extensión en el uso del correo electrónico,

[151] Estados Unidos Apuesta por el Comercio Electrónico, 4 de julio del 2000, Mercedes Asorev, http://www.expansiondirecto.com/2000/07/04/tecnologia/4tec.html.

[152] Rodolfo Gasparri, Internet Banking será el Canal de Distribución por Excelencia, Abril/Mayo 2000, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

computadoras, fibra óptica e Internet cambiara la manera de trabajar, aprender y hacer negocios"[153] .

Un ejemplo de esto es que desde "los atentados del 11 de setiembre en Nueva York abrieron una ventana de oportunidad para este negocio, pues ahora para muchos ejecutivos piensan dos veces antes de viajar, por lo que Internet se ha convertido en una herramienta para hacer negocios."[154]

d.- Mensajería Electrónica:

"La nueva economía se basa en la inteligencia de la red. "Ahora la información en todas sus formas es digital, reducida a bits almacenados en computadores, desplazándose a la velocidad de la luz, a través de las redes, de esta manera, el nuevo mundo de las posibilidades creadas, es tan significativo como la invención del lenguaje". De allí que nos encontremos frente a un nuevo esquema de procesos de transacción, con base en la nueva economía, donde el

[153] Rodolfo Gasparri, Internet Banking será el Canal de Distribución por Excelencia, Abril/Mayo 2000, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

[154] ***Édgar Delgado M.,*** Gran potencial en Internet. ***Abrirán certificadora de firmas digitales,*** Lunes 3 de diciembre, 2001. San José, Costa Rica, www.Lanacion.com

cerebro humano, en lugar de la fuerza física, creará cada vez mayor valor agregado."[155]

Es así como la mensajería electrónica figura como medio para realizar toda clase de negocios, transacciones, contratos y aplicación de servicios, creando está, una nueva forma de comunicarnos, contratar y hacer efectivas múltiples transacciones en beneficio de nuestra economía.

Como ejemplo de esto tenemos: "los procesos de transferencias en dólares e instrumentos financieros a plazo desde la perspectiva de dos canales de distribución diferentes: las oficinas e Internet, indicando que a través de Internet, no sólo se reducen los costos, sino también el tiempo del proceso."

Dentro de la mensajería es importante comprobar los datos personales del emisor o receptor a fin de situarlo dentro del contexto legal y comprobar su identidad, para que sus actos sean válidos y eficaces.

Es por todo lo anterior que la mensajería figura parte esencial del desempeño efectivo y real de la firma digital, logrado con estos múltiples beneficios.

---

[155] Rodolfo Gasparri, Internet Banking será el Canal de Distribución por Excelencia, Abril/Mayo 2000, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

e.- Banca:

A pesar de que este punto esta incluido dentro de los servicios financieros del inciso b, debido a su importancia y utilización se ha desarrollado una forma más especifica como un punto aparte.

"Actualmente, Banco Mercantil realiza 500.000 transacciones bancarias vía Internet y algunos clientes reciben por correo electrónico sus estados de cuenta."[156] Este es sólo el inicio del desarrollo de la firma digital dentro de las transacciones bancarias.

No obstante las facilidades de "comunicación han permitido que los negocios marchen a un ritmo diferente, utilizando a los bancos y las tarjetas de crédito como soporte de las transacciones, y pronto incorporarán a este nuevo concepto, las tarjetas de débito y el monedero electrónico, convirtiéndose el banco en la infraestructura del comercio electrónico. Los nuevos canales de comercialización y acceso al servicio bancario están desbancando a las tradicionales sucursales. Los cajeros, la banca telefónica, Internet, la telefonía móvil y, últimamente, la televisión digital, se suman a esta lista de ventanas

[156] Rodolfo Gasparri, Internet Banking será el Canal de Distribución por Excelencia, Abril/Mayo 2000, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

a través de las que es posible contactar con una entidad financiera."[157]

Es por esto que a nivel bancario se necesita un mecanismo que obligue a que los datos bancarios relacionados con el pago on-line, o alguna otra transacción confidencial se haga directamente a una entidad bancaria haciendo imposible la intrusión de terceros que no tienen ninguna relevancia dentro del proceso.

La seguridad total es parte importante de este punto, sobre todo cuando se habla de dinero o pagos a la entidad bancaria. Debido a la cantidad de espías en la red cada vez se va haciendo más importante mantener un grado de seguridad mayor, en el caso del banco por la gran cantidad de clientes que puede poseer lo más recomendable sería que los clientes obtengan un certificado que sea expedido por el propio banco.

f.- Comercio Electrónico:

Este "no solo incluye la compra y venta electrónica de bienes o servicios, que es el concepto común que se tiene, sino que también incorpora el uso de redes para actividades anteriores o posteriores a la venta, como son: la publicidad, la búsqueda de información, el

[157] Rodolfo Gasparri, Internet Banking será el Canal de Distribución por Excelencia, Abril/Mayo 2000, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

aseguramiento de las posibles transacciones, el tratamiento de clientes y proveedores, incluso inversores, trámites ante autoridades de control y fiscalización, la negociación de condiciones de compra, suministro, etc., la prestación de mantenimiento y servicios posventa y la colaboración entre las empresas."[158]

"El mercado electrónico está referido al mercado económico que se encuentra en crecimiento, en donde los productores, intermediarios y consumidores interactúan de alguna forma electrónica o por intermedio de un contacto digital. Los mercados físicos son representados de forma virtual en el mercado electrónico y la economía digital se encuentra representada por medio de las actividades económicas a cargo de este mercado electrónico."[159]

Es aquí donde considero se va a desempeñar en una mayor forma la figura de la firma digital, donde diversos individuos de distintas partes del mundo desean contratar y realizar múltiples negocios.

---

[158] DE PALADELLA SALORD (Carlos), El Dinero físico y su desaparición?, Argentina, 1999. Documento de internet disponible: http://www.publicaciones.derecho.org/redi/index.cgi?/N%Famero_10_-Mayo_de 1999/paladella.

[159] Jesús María, **Instituto Nacional de Estadística e Informática, ¿QUÉ ES EL COMERCIO ELECTRÓNICO?http://www.uap.edu.pe/fac/02/enlaces/manualhtmlegl/inei/Libro-5104.pdf**

Al existir una figura regulada de la firma digital se da más seguridad y tranquilidad a los individuos, los cuales en lugar de trasladarse de un lugar a otro para comerciar o negociar sus productos, realizan todas sus transacciones desde la comodidad de su casa u oficina, ahorrando tiempo y dinero los cuales son de mucha importancia para cualquier persona pero en especial para un comerciante[160].

g.- Servicios Administrativos:

En cuanto a estos tenemos que hacer alusión a lo estipulado por el señor Roberto Soto, Gerente de Desarrollo de Negocios de Antisoft en el periódico el financiero, respecto a la aplicación del "Gobierno Digital"[161] el cual dice: "El gobierno digital nos cambiará la vida a

[160] Cuando se habla de comerciante como en este caso en particular es importante recordar lo dispuesto en el artículo 5 del Código de Comercio de la República de Costa Rica, Porvenir 1999, el cual dice que son comerciantes: a)Las persona con capacidad jurídica que ejerzan en su nombre propio actos de comercio, haciendo de ello su ocupación habitual; b) Las empresas individuales de responsabilidad limitada; c)Las sociedades que se constituyan de conformidad con disposiciones de este Código, cualquiera sea el objeto o actividad que desarrollen; d) Las sociedades extranjeras y las sucursales y agencias de estas, que ejerzan actos de comercio en el país, sólo cuando actúen como distribuidores de los productos fabricados por su Compañía en Costa Rica; y e) Las sociedades de centroamericanos que ejerzan el comercio en nuestro país.

[161] Roberto Sasso, Gerente de Desarrollo de Negocios Antisoft, 26 de mayo 1 de junio del 2003, Urge el Gobierno Digital, El Financiero define El gobierno digital como: "un conjunto de tecnologías basadas en los estándares de Internet y que permite mejorar los servicios estatales y reducir los costos la mismo tiempo." Pág. 8

todos: simplificará, abaratará y facilitará nuestra relación con el Estado."[162]

Es tan simple como él lo estipula, evitar filas innecesarias, exceso de personal, gastos en papelería y utensilios de oficina simplifica y abarata los costos de todo además de brindar un servicio más rápido y eficiente son parte de lo que podría generar la firma digital y es que no sólo podemos encasillarnos en el comerciante.

Indiscutiblemente el estado y por ende sus funcionarios deben ser parte de este cambio y este beneficio tan grande como lo es la firma digital.

No tendríamos que trasladarnos para realizar nuestras declaraciones de renta, ni para revisar un expediente médico, ni judicial del cual soy parte interesado, estas son muchas de las ventajas que puedo obtener involucrando al Estado.

Asimismo, el Estado podría realizar actividades tanto nacionales como internacionales, que le generen ingresos (transacciones comerciales) o le disminuyan gastos (contratación, pagos, etc.) con la utilización de la firma digital.

[162] Roberto Sasso, Gerente de Desarrollo de Negocios Antisoft, 26 de mayo 1 de junio del 2003, Urge el Gobierno Digital, El Financiero, Pág. 8

h.- Educación a Distancia:

Hoy en día son muchos los que estudian utilizando Internet, cada vez son más los cursos, licenciaturas y doctorados que se realizan en otro país vía Internet, donde las clases presenciales desaparecen y por el contrario el desarrollo de una conciencia de estudio aumenta.

Con este sistema puedo realizar mis exámenes asegurando que la persona quien los hace es quién realmente dice ser, así como si mi consulta es evacuada por mi profesor designado y debidamente preparado para contestar la misma.

Los gastos de hospedaje, alimentación, papelería y demás que pueda generarse del traslado a otro país para estudiar, no son necesarios, y por tanto los costos de mis estudios también bajaran.

i.- Trabajo Cooperativo:

Muchos de los problemas de las pequeñas y medianas empresas para lograr un mayor desarrollo es la falta de capital, no obstante por medio de la firma digital puedo asegurarme de la responsabilidad que pueda existir de asociarme a otra empresa la cual me ayude a desempeñar de una mejor forma mi negocio.

Por ejemplo, La Candela Feliz es una empresa pequeña que se dedica a confeccionar y vender candelas, el problema que tiene es que el costo de la parafina con la que confecciona las candelas es muy caro en Costa Rica, La Candela Felíz descubre que en Holanda en La Casa de la Candela, la parafina que necesita tiene un precio por debajo del 50% del precio. No obstante el traslado hasta Holanda es muy alto, por lo que decide obtener un certificado digital y contactar a La Casa de la Candela en Holanda vía Internet, realiza la transacción y como La Casa de la Candela en Holanda también tiene certificado digital se asegura que su orden de compra sea correcta y que la respuesta a la misma orden de compra sea eficaz y segura.

Ambas empresas poseen obligaciones y responsabilidades, debido a que la firma digital contenida en el certificado digital, tiene la característica de ser auténtica, integra y no repudiable, en consecuencia el negocio se realiza de forma eficaz, debido a la cooperación de ambas.

En conclusión La Casa de la Candela gana más porque ya puede vender la parafina internacionalmente, y La Candela Felíz puede hacer y vender más candelas manteniendo su calidad y

bajando sus costos, por consiguiente puede bajar los precios de la candela logrando un beneficio para todos.

SECCIÓN TERCERA: APLICACIONES EN PARTICULAR SOBRE LA FIRMA DIGITAL Y EL DOCUMENTO ELECTRÓNICO FIRMADO DIGITALMENTE.

Además de las aplicaciones generales, El Lic. Daniel Edgardo Cortés, considera en su trabajo de Aplicaciones en Particular Sobre la Firma Digital[163], que existen diversas aplicaciones sobre la firma digital y otras en especial sobre el documento digital firmado digitalmente que son las siguientes:

a.- Aplicaciones en Particular Sobre la Firma Digital.

- Firma y/o Cifrado de Correo Electrónico, tanto Interno como Externo.
- Firma y/o Cifrado de Documentos (Pericias, Dictámenes, Planos, Software, Políticas, Procedimientos, Normativas, Minutas, y otros).
- Identificación de Personas ante Sistemas Internos en redes locales y abiertas (Intranets), Sitios Web (sin necesidad de registrar datos). Determinación implícita del Perfil de Usuario. · Identificación de Sistemas ante el Usuario (¿Cómo sé que es el

[163] Lic. Daniel Edgardo Cortés, Aplicaciones en particular sobre la firma digital, **www.certificadodigital.com.ar**, http://www.fundaciondike.org/seguridad/firmadigital.html

sistema que dice ser?).

• Auditoría de Transacciones.

• Seguridad al operar Comercialmente (Compra-Venta de Acciones, Transacciones Bancarias, Operaciones con Tarjeta de Crédito, y otras).

• Identificación de los componentes físicos de una red (Computadores, Ruteadores, Teléfonos Celulares, y otros).

• Mediciones realizadas por instrumental electrónico que deba ser corroborado por un especialista.

b.- Aplicaciones en Particular Sobre el Documento Electrónico Firmado Digitalmente

• Fidelización de Documentos digitalizados.

• Cotizaciones de Bienes y Servicios (tanto el pedido como la cotización y condiciones del Proveedor).

• Resúmenes de Cuenta.

• Recibos de Pago.

• Adjudicaciones.

• Factura Electrónica.

• Cheque Electrónico.

• Invitaciones.

- Promociones.
- Acreditaciones de Puntaje.
- Remitos de Entrega.
- Órdenes de Compra.
- Solicitudes de Adhesión.
- Contratos.
- Actas.
- Planos.
- Planificaciones.
- Circulares internas y/o externas.
- Reservas o Turnos para distintas prestaciones (Talleres, Médicos, Hoteles, Pasajes, etc.).
- Confirmaciones.
- Autorizaciones de Prestaciones Médicas.
- Receta Médica Electrónica.
- Historia Clínica única.
- Declaraciones Juradas.
- Solicitudes de Prestación de Servicios.
- Proyectos.
- Diseños.

- Tarjetas de Crédito (sin utilizar el número y consecuentemente disminuir el fraude).
- Entre otros.

TÍTULO TERCERO

ANÁLISIS DEL PROYECTO DE LEY 14276, "LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES", JUNTO A DOCTRINA Y EXPERIENCIA COMPARADA.

CAPÍTULO PRIMERO.

CONSIDERACIONES SOBRE EL PROYECTO DE LEY 14276 "LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES".

SECCIÓN PRIMERA: DOCTRINA APLICABLE.

a.- PRINCIPIOS, CONSTITUCIÓN POLÍTICA Y LEYES.

- **Principio de Neutralidad Tecnológica:** este principio es sumamente importante debido a que procura que la normativa no límite el mecanismo de firma digital a una sola tecnología.

Asimismo, establece reglas mínimas para que se puedan desarrollar diversas tecnologías.

- **Principio de celeridad y eficacia:** implica un proceso necesariamente rápido, eficaz y confiable.

Este es uno de los pilares de la firma digital debido a que la misma se desarrolla con base en estos principios, manteniendo la confianza, seguridad e integridad de esta figura.

- **Principio de equivalencia funcional de la firma digital:** busca que la firma digital satisfaga los requerimientos de la firma en los

datos consignados en forma electrónica, teniendo la firma digital los mismos efectos jurídicos que la firma manuscrita en relación a lo signado.

- **<u>Constitución Política de Costa Rica:</u>**

"ARTÍCULO 24.- *Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.*

Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de

inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial."[164]

Este artículo en aplicación a la firma digital es muy importante, debido a que la constitución es la base de toda nuestra normativa, por esto considero que la firma digital debe ser aplicada al amparo de este artículo, debido a que la misma es una manifestación de voluntad que debe ser protegida, garantizándole a los ciudadanos el derecho a la libertad, la intimidad y el secreto de las comunicaciones.

A su vez, brinda seguridad a todos los individuos, garantizando que en los casos que corresponda las autoridades podrán intervenir y resolver de conformidad con el debido proceso, el problema o la ilegalidad en la que se haya incurrido.

- **Código de Comercio:**

"ARTÍCULO 414.- *La Firma reproducida por algún medio mecánico no se considera eficaz, salvo los negocios, actos contratos en que la ley o el uso admitan,*

[164] Lic. Marco Rojas Castillo, Constitución Política de Costa Rica, Uruck Editores, 1996, Cartago Costa Rica.

especialmente cuando se trate de suscribir valores emitidos en número considerable."[165]

Este es uno de los artículos que deberá modificarse, debido a que se entiende que la firma digital es reproducida por medios mecánicos como lo son las computadoras. Asimismo, la firma digital pretende incursionar en todos los mercados no solo para suscribir valores, por lo que no podríamos dejar el uso de estas nuevas tecnologías a un área tan pequeña como lo señala este artículo.

- **Código Civil:**

"**ARTÍCULO 1008.-** *El Consentimiento de las partes debe ser libre y claramente manifestado.*

La manifestación puede ser de palabra, por escrito o por hechos de que necesariamente se deduzca."[166]

En la firma digital el consentimiento se ve un poco diferente al utilizado durante varias décadas, no obstante debemos entender que siempre dicho consentimiento se mantiene y este se manifiesta al insertar la clave privada que identifica a la firma digital, para realizar

[165] Art.414 del Código de Comercio, 15 Edición, 1999, Editorial Porvenir

[166] Artículo 1008 del Código Civil, 8 Edición, 2001, Editorial Investigaciones Jurídicas.

un contrato o cualquier otro acto que se derive de las relaciones ya sea comerciales o no comerciales entre los individuos.

Dicho consentimiento en la firma digital es libre y claramente manifestado es por esto que la firma se considera un prueba válida y eficaz para juicio.

- **Código Procesal Civil:**

"**ARTÍCULO 368.-** *Distintas clases de documentos: Son documentos los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y, en general, todo objeto mueble que tenga carácter representativo o declarativo*."[167]

La firma digital posee carácter declarativo debido a que es parte de las diversas manifestaciones de voluntad que realizan los individuos, declarando su deseo de continuar con una operación, perfeccionar un escrito y hasta contratar.

Es así como los documentos firmados digitalmente entran dentro de lo expuesto en el anterior artículo, siendo un bloque de caracteres

[167] Artículo 368, Código Procesal Civil, 8 Edición, setiembre 1999, Editorial Investigaciones Jurídicas S.A.

que acompañan al documento, acreditando quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad).

- **Código Notarial:**

"ARTÍCULO 3.- *Requisitos: Para ser notario público y ejercer como tal, deben reunirse los siguientes requisitos:*

a) Ser de buena conducta.

b) No tener impedimento legal para el ejercicio del cargo.

c) Ser licenciado en Derecho, con el postgrado en Derecho Notarial y Registral, graduado de una universidad reconocida por las autoridades educativas competentes; además, haber estado incorporado al Colegio de Abogados de Costa Rica al menos durante dos años y, con la misma antelación, haber solicitado la habilitación para ejercer el cargo.

d) Poseer residencia fija en el país, salvo los notarios consulares.

e) Tener oficina abierta al público en Costa Rica, excepto si se trata de notarios consulares.

f) Hablar, entender y escribir correctamente el español.

Los extranjeros que cumplan con los requisitos anteriores podrán ejercer el notariado siempre que en su país de origen se otorgue el mismo beneficio a los notarios costarricenses, en igualdad de condiciones."[168]

Este artículo nos habla de la función notarial, no obstante a raíz del desarrollo de la tecnología este ha ido cambiando radicalmente hasta el punto de casi tener que solicitar no solo tener la oficina abierta, sino también los medios electrónicos para poder contactársele. Asimismo, con el desarrollo de la firma digital es importante recordar que esta podrá ser utilizada por los y las notarias, para autenticar por medio de su clave privada documentos, por lo tanto debería de requerírsele a cada notario la obtención de la misma siempre y cuanto ostenten los requisitos necesarios para obtenerla.

"ARTÍCULO 110.- *Potestad certificadora: Los notarios podrán extender, bajo su responsabilidad, certificaciones relativas a inscripciones, expedientes, resoluciones o documentos existentes en registros y oficinas públicas, así como de libros, documentos o piezas privadas en poder de particulares. Para este fin, pueden utilizar fotocopias.*

[168] Art. 3 sobre la función notarial, Código Notarial Ley N°7764 de 17 de abril de 1998 y sus reformas.

En todo caso es necesario indicar si el documento se certifica literalmente, en lo conducente o en relación.

Si lo certificado fueren documentos privados, el notario debe dejar copia auténtica en el archivo de referencias, con indicación del solicitante y de la hora y fecha en que se expidió.

En estas certificaciones, podrán corregirse errores materiales o subsanarse omisiones en la pieza original y en las protocolizaciones, lo cual debe advertirse.

Siempre deben satisfacerse las especies fiscales correspondientes, los timbres o derechos que deban cubrirse, como si las certificaciones fueran expedidas por la oficina o el registro donde constan las piezas originales. Para todos los efectos legales, esas certificaciones tendrán el valor que las leyes conceden a las extendidas por los funcionarios de dichas dependencias, mientras no se compruebe, con certificación emanada de ellos, que carecen de exactitud sin que sea necesario, en este caso, argüir falsedad.

El notario que en dichas certificaciones consigne datos falsos, aparte de las responsabilidades penales y civiles, será sancionado disciplinariamente.

En las certificaciones de documentos privados en poder de particulares será aplicable, en lo pertinente, el artículo 107."[169]

Este artículo debe ser modificado debido que con el inicio de la firma digital los documentos certificados también serán documentos electrónicos por lo que el notario deberá tener un soporte electrónico confiable para almacenar los mismos.

Ya no solo se certificará las copias de los documentos, o algún otro documento privado, sino que podrá certificar hasta actuaciones. Lo que se pretende es evitar los gastos materiales y garantizar de una forma más efectiva la actuación de los notarios.

"ARTÍCULO 111.-*Autenticación de firmas y huellas digitales: El notario podrá autenticar firmas o huellas digitales, siempre que hayan sido impresas en su presencia; para ello debe hacer constar que son auténticas. Del mismo modo se procederá cuando una persona firme a ruego de otra que no sabe o no puede hacerlo; en este caso, debe firmar en presencia del notario.*

Los documentos privados en que se practiquen autenticaciones, conservarán ese mismo carácter."[170]

---

[169] Art. 110 Potestad Certificadora, Código Notarial Ley N° 7764 de 17 de abril de 1998 y sus reformas.

[170] Art. 111 Autenticación de huellas y firmas digitales, Código Notarial Ley N° 7764 de 17 de abril de 1998 y sus reformas.

En lo que respecta a documentos electrónicos este artículo no aplicaría, debido a que si envío un documento electrónico a un notario para que este autentique mi firma, con el fin de darle más validez (el notario estaría haciendo la función de autoridad certificadora), la persona que envía dicho documento no lo está firmando en mí presencia. No obstante las características principales de la firma digital es su autenticidad, integridad y no repudio, esto se debe a que la persona ya sea física o jurídica posee una clave pública y otra privada, la cual solo él o ella tiene conocimiento de la misma, asegurando de esta forma que efectivamente se trata de quién dice ser.

- **CÓDIGO PENAL**

"ARTÍCULO 196 BIS.- *"Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."*

ARTÍCULO 217 BIS.- *"Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."*

ARTÍCULO 229 BIS.- *"Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.*

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

Estos artículos son una de las últimas innovaciones que ha tenido nuestro Código Penal en esta materia cuyo fin es tutelar de una mejor forma la intimidad y el secreto a las comunicaciones así como la integridad y confiabilidad de un documento o programa.

- **LEYES DE LA REPÚBLICA DE COSTA RICA.**

Ley del Sistema Nacional de Archivos No. 7202:

"ARTÍCULO 3.- *Todos los documentos con valor científico cultural son bienes muebles y forman parte del patrimonio científico cultural de Costa Rica. La determinación del valor científico-cultural del documento corresponderá a la Comisión Nacional de Selección y Eliminación de Documentos.*

Se consideran de valor científico-cultural aquellos documentos textuales, manuscritos o impresos, gráficos, audiovisuales y legibles por máquina que, por su contenido, sirvan como testimonio y reflejen el desarrollo de la realidad costarricense, tales como: actas, acuerdos, cartas, decretos, informes, leyes, resoluciones, mapas, planos, carteles, fotografías, filmes, grabaciones, cintas magnéticas, "diskettes", y los demás que se señalen en el reglamento de esta ley."[171]

Esta ley pone en evidencia nuestro intento por realizar un cambio tecnológico e ir incorporando a nuestra legislación y sistema, nuevas tecnologías que faciliten la concepción del documento de una manera mucho más amplia, abriendo las puertas a un mundo lleno de cambios tecnológicos que obligan a los individuos a cambiar no solo estructuralmente sino también mentalmente sus comportamientos, actos, contratos entre muchas otras cosas más.

[171] Artículo 3 de la Ley del Sistema Nacional de Archivos No. 7202, 24 de Octubre de 1990.

La Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, Nº 7425:

"ARTICULO 1.-*Competencia. Los Tribunales de Justicia podrán autorizar el registro, el secuestro o el examen de cualquier documento privado, cuando sea absolutamente indispensable para esclarecer asuntos penales sometidos a su conocimiento. Para los efectos de esta Ley, se consideran documentos privados: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo*."[172]

Es así como sigue surgiendo nuestro derecho, hasta el punto de aceptar las distintas formas de registrar información como posibles fuentes de evidencia que ayuden a esclarecer un problema. Al incorporar dentro de este artículo, nuevas tecnologías lo que se busca es cumplir con el principio anteriormente mencionado "Principio de Neutralidad Tecnológica".

[172] Artículo 1 de la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, Nº 7425, 9 de agosto de 1994

No obstante lo limita a asuntos penales solamente, sin que se pueda aceptar o atribuir para otra clase de asuntos como bien podrían ser los procesos ordinarios, ejecutivos, etc.

La Ley Orgánica del Poder Judicial con la reforma introducida por la Ley Nº 7728:

"ARTÍCULO 6 bis.- *Tendrán la validez y eficacia de un documento físico original, los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos o producidos por nuevas tecnologías, destinados a la tramitación judicial, ya sea que contengan actos o resoluciones judiciales. Lo anterior siempre que cumplan con los procedimientos establecidos para garantizar su autenticidad, integridad y seguridad. ...*"[173]

Este artículo es sumamente importante, debido a que marca una pauta muy grande dentro del Poder Judicial, logrando facilitar y mejorar la eficacia en los trabajos realizados por esta autoridad.

No obstante presenta el mismo problema del artículo analizado anteriormente: limita la validez y eficacia de un documento, debido a que le atribuye estos valores únicamente a aquellos que hayan sido destinados para la tramitación judicial.

[173] Artículo 6 bis, de la Ley Orgánica del Poder Judicial con reforma introducida por la ley Número 7728, 15 de diciembre de 1997.

Ley General de Aduanas y su Reforma Proyecto de Ley N° 15.007.

Existe un Proyecto de Ley en la Asamblea Legislativa denominado Ley General de Aduanas y su Reforma, expediente número 15.007, el cual pretende reformar varios artículos de esta ley, de los cuales considero importantes mencionar brevemente, debido a su vínculo con el tema que hemos estado desarrollando (la negrita en los siguientes artículos no es original):

"**ARTICULO 103.-** *Informatización de los procedimientos. Cuando la Dirección General de Aduanas lo determine mediante resolución de carácter general, y le asigne clave de acceso confidencial y código de usuario correspondiente* ***o su certificado digital mediante un prestador de servicios de certificación,*** *el auxiliar de la función pública aduanera deberá realizar los actos correspondientes conforme a esta Ley y sus Reglamentos, empleando el sistema informático de conformidad con los formatos y las condiciones autorizadas.*

***Las firmas autógrafas que la misma requiera podrán ser sustituidas por contraseñas o signos adecuados, como la firma electrónica, para la sustanciación de las actuaciones administrativas que se realicen por medios informáticos.*"**

"ARTÍCULO 104.- *Declaración por transmisión electrónica de datos. El declarante o agente aduanero que lo represente debe presentar la declaración mediante transmisión electrónica de datos, utilizando su código de usuario y clave de acceso confidencial* ***o firma electrónica*****."**

"**ARTÍCULO 105.-** *Código y clave de acceso o firma electrónica. Los funcionarios, auxiliares de la función pública aduanera y demás usuarios, serán responsables del uso del código de usuario y de la clave de acceso confidencial o firma electrónica asignados y de los actos que se deriven de su utilización.*

La clave de acceso confidencial y/ o firma electrónica equivale a la firma autógrafa de los funcionarios, auxiliares y demás usuarios, para todos los efectos legales."

"ARTÍCULO 106.- *Prueba de los actos realizados en sistemas informáticos. Los datos y registros recibidos y anotados en el sistema informático, constituirán prueba de que el auxiliar de la función pública aduanera realizó los actos que le corresponden y que el contenido de esos actos y registros fue suministrado por este, al usar la clave de acceso confidencial o la firma electrónica.*

Los funcionarios o las autoridades que intervengan en la operación del sistema serán responsables de sus actos y de los datos que suministren, ***según las formalidades requeridas y dentro del límite de sus atribuciones; actos que***

constituirán instrumentos públicos y como tales se tendrán como auténticos. *Cualquier información transmitida electrónicamente por medio de un sistema informático autorizado por la Dirección General de Aduanas, será admisible en los procedimientos administrativos y judiciales como evidencia de la transmisión de esa información…***"**

"**ARTÍCULO 266.-** *Definiciones. Para la aplicación de esta Ley, se definen los siguientes conceptos:*

[...]

CERTIFICADO DIGITAL: *Documento firmado electrónicamente por el prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.*

[...]

FIRMA ELECTRÓNICA: *Resultado de obtener, por medio de mecanismos o dispositivos, un patrón que se asocie unívocamente a una persona física o jurídica y a su voluntad de firmar.*

[...]

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN: *Persona física o jurídica, pública o privada, que expide certificados o presta otros servicios en relación con la firma electrónica.*"

En este proyecto en general debemos ver claramente, que se confunden los términos de firma electrónica y firma digital, debido a que se asocia la firma electrónica con una contraseña lo cual es incorrecto y deberá analizarse dentro de este proyecto en el momento de discusión en la Asamblea Legislativa.

No obstante, además de lo anterior debemos observar que la firma se necesita en múltiples áreas, una de estas es la aduanera, cuyos interesados han manifestado a viva voz su deseo de ser parte de un nuevo cambio en la legislación.

Dentro de estos artículos se hace referencia a la existencia y aplicación de los certificados digitales, los prestadores de certificación, se autoriza y a la vez se le otorgan obligaciones y responsabilidades al agente aduanero a la hora de utilizar lo que ellos denominan la firma electrónica.

Deja ver el carácter confidencial de la firma electrónica, otorgando al signatario facilidades para desenvolverse en sus labores diarias.

No obstante lo anterior, vemos como en su artículo 266 define de una forma confusa e incorrecta los términos, pudiendo estos causar problemas a futuro.

Recordemos que:

Un **Certificado digital** *es una estructura de datos empleada dentro de un sistema de clave pública para ligar una persona determinada con una clave privada única, los certificados lo que permiten es verificar si los datos consignados corresponden al individuo determinado, ayudando a evitar que alguien utilice una clave falsa y se haga pasar por otra persona.*

Por consiguiente el certificado no es firmado mucho menos electrónicamente por el prestador de servicios de certificación.

La **Firma Electrónica** "*es cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente su autor.*"[174]

Por lo que es muy diferente al que se utiliza en este proyecto debido a que la firma electrónica no está ligada a una clave confidencial, y mucho menos podrá asociarse unívocamente a una

[174] Revista de Ciencias Jurídicas #97, Comercio Electrónico un breve acercamiento, Dr. Jorge Enrique Romero Pérez, Pág.123Facultad de Derecho enero-abril-2002.

sola persona debido a que fácilmente puede ser confeccionada por cualquiera que conozca la cantidad mínima de caracteres.

b.- RESOLUCIONES DE SALA DE LA CORTE SUPREMA DE JUSTICIA.

Sala Constitucional, Voto Nº 3495 de las catorce horas treinta minutos del diecinueve de noviembre de mil novecientos noventa y dos, sobre las libertades contractuales.

La acción se promueve por considerarse que el artículo 6 de la Ley de la Moneda viola lo dispuesto en los 7, 10, 27, 41, 45 y 46 de la Constitución Política y 8 de la Convención Americana sobre Derechos Humanos.

Es así como se realiza todo un análisis a las libertades de las personas y formas de pactar determinándose al final que dicho artículo 6 debería ser modificado y leído de la siguiente forma:

ARTÍCULO 6.-

"En toda determinación de precios, fijación de sueldos, jornales, honorarios, pensiones y toda clase de remuneraciones, indemnizaciones o prestaciones, imposición de derechos, impuestos y contribuciones, y en cualesquiera otras obligaciones públicas

o privadas, que impliquen empleo de dinero y deban solventarse en Costa Rica, los importes correspondientes deberán necesariamente expresarse en colones.

Sin embargo, podrán celebrarse contratos y contraerse obligaciones en monedas extranjeras, pudiendo, a opción del deudor, cancelarse en colones".

Esta reforma es importante para el desarrollo de la firma digital, debido a que como hemos ido analizando la firma digital puede ser usada para múltiples transacciones entre distintos individuos, ya sea dentro del mismo país o fuera de él, por lo que es esencial conocer como deberá consignarse y cancelarse el pago o remuneración que se dé producto de los servicios y/o labores brindadas ya sea utilizando medios electrónicos o tradicionales.

c.-OTROS PRONUNCIAMIENTOS.

Procuraduría General de la República, C-283-98 de 24 de diciembre de 1998, elaborado por el Procurador Enrique Germán Pochet Cabezas, acerca de la firma digital y los documentos electrónicos.

Este pronunciamiento hace referencia a una serie de aspectos importantes, surgió de la consulta de la Licda. Ana Virginia García de

Benedicts, sobre la validez del documento "escrito" en disco óptico (CD-ROM), a la cual respondió el Lic. Enrique Germán Pochet Cabezas.

Después de realizar los análisis jurídicos afines "tales como el almacenamiento computarizado de la información, la lectura y escritura informática, los discos magnéticos y los compactos, el concepto de documento (continente y contenido), su definición, la evolución de documento en nuestro derecho positivo, el documento electrónico y su autenticidad, las firmas digital y digitalizada, el valor probatorio del documento, junto con las regulaciones archivísticas y la Ley del Archivo Nacional…"[175], haciendo referencia a los anteriormente mencionados y analizados artículos 368 del Código Procesal Civil, artículo 1 de la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, artículo 6 bis de la Ley Orgánica del Poder Judicial y el artículo 3 de la Ley del Sistema Nacional de Archivos.

[175] Procuraduría General de la República, C-283-98 de 24 de diciembre de 1998, elaborado por el Procurador Enrique Germán Pochet Cabezas, acerca de la firma digital y los documentos electrónicos, Pág. 22.

En dicho pronunciamiento se llegó a la conclusión de que el disco compacto constituye un documento con valor jurídico en nuestro ordenamiento jurídico.

Por lo tanto, le corresponde al "Archivo Nacional establecer las políticas y dictar las regulaciones específicas para permitir la recuperación y actualización de este instrumental tecnológico que contemplen los requisitos técnicos, archivisticos y administrativos, para que la producción de tal acervo pueda efectivamente cumplir y garantizar su función documental."[176]

[176] Procuraduría General de la República, C-283-98 de 24 de diciembre de 1998, elaborado por el Procurador Enrique Germán Pochet Cabezas, acerca de la firma digital y los documentos electrónicos, Pág. 21.

SECCIÓN SEGUNDA: ANÁLISIS DEL ARTICULADO DEL TEXTO 14276 "LEY DE FIRMAS Y CERTIFICADOS DIGITALES"[177] ULTIMA VERSIÓN.

a.- TÍTULO PRIMERO: DISPOSICIONES GENERALES.

De conformidad con el transcurso del tiempo el proyecto se ha ido modificando paulatinamente, hasta llegar a una versión bastante amplia y distinta de la original.

En el proyecto considero se debe mantener una uniformidad en cuanto al articulado de manera que se nombre a una entidad de una sola forma esto con el fin de evitar posibles confusiones en la aplicación del texto.

Me llama particularmente la atención que en el texto se habla de Prestador de servicios de certificación o entidades de certificación, a pesar de que estas muchas veces en la normativa internacional se definen como instituciones apartes.

Es por esto que considero que debe de utilizarse sólo un término de estas no ambas, en la normativa tan específica como es este texto.

A pesar de que dicho proyecto se ha ido modificando, continúan existiendo lagunas y deficiencias en el articulado de este.

[177] Los artículos que se consignan aquí son tomados de la Unidad de Asuntos Jurídicos, Asamblea Legislativa, Proyecto de ley 14276.

Las siguientes son observaciones al articulado del proyecto:

ARTÍCULO 1.- En general considero que el objeto está correcto. Sin embargo debe analizarse si la firma digital va a ser aplicada a todos los casos sin excepción.

Algunas países como en Guatemala, han decidido incorporar la firma digital a su país, pero limitando algunos actos, es así como observamos que la "Ley para la promoción del Comercio Electrónico y Protección de la Firma Digital" en su artículo primero estipula "La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los casos siguientes:

a) En las obligaciones contraídas por el Estado en virtud de Convenios o Tratados Internacionales.

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo."[178]

ARTÍCULO 2.- En este artículo se definen muchos términos que crean confusiones o están mal empleados los cuales analizaremos.

[178] Proyecto de Ley para la Promoción del Comercio Electrónico y Protección de la Firma Digital, El Congreso de la Republica de Guatemala.

Asimismo deben incluirse dentro de esta lista taxativa de definiciones otras que garanticen la débida aplicación y entendimiento de la ley.

En lo que concierne a las definiciones utilizadas en este capítulo considero que:

Inciso 1: **ACREDITACIÓN**, es cierto que el reconocimiento debe ser formal para brindar mayor seguridad jurídica y confiabilidad, sin embargo no sólo deberá reconocer a una entidad o empresa, debe ser más abierta, incorporando a este párrafo: "… reconoce formalmente que una persona física, jurídica, pública o privada es competente para realizar las tareas de certificación digital…"

Inciso 2: **ACREDITACIÓN VOLUNTARIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN**, entremos a analizar el término "voluntario" se define como: "La aceptación o negativa de un sujeto que la ley predetermina, de no constar; o que se conjetura de no conocerse…Potencia o facultad de alma que lleva a obrar o abstenerse…"[179]

Si bien es cierto que la voluntad, implica un consentimiento, al incluir el término voluntario en este artículo hace que surja la duda de

[179] Diccionario Jurídico Elemental, Guillermo Cabanellas, Edición 1998, Editorial Heliasta.

si existe o no, una acreditación obligatoria para una determinada persona ya sea física, jurídica, privada o pública.

Además por más voluntad o deseo que tenga de acreditarme para realizar tareas de certificación digital, este no puede ser el único requisito para constituirme como tal.

En este mismo artículo se hace referencia a una resolución, considero que dicho término debería de cambiarse por un término menos amplio.

Recordemos que la firma digital se utilizará tanto a nivel nacional como internacional, y que el término resolución puede catalogarse como ambiguo.

Debemos tomar en cuenta que con el transcurso del tiempo los términos cambian, si bien es cierto, está definición es muy similar a la estipulada en el Real Decreto- Ley Español. No obstante debemos procurar crear nuestra normativa, evitando errores que en otros países han cometido al regular esta figura.

Inciso 4: **CERTIFICADO DIGITAL RECONOCIDO**, en general la redacción es confusa. No se sabe si se va a vincular la firma digital con el signatario o con la entidad.

El concepto debe darse más claro, lo cual no significa que hay que cambiarlo del todo, con sólo eliminar algunas palabras puede corregirse veamos: "Certificado Digital Reconocido: es el certificado digital que cumple con los requisitos establecidos en la presente ley y su reglamento, vinculando una firma digital con su signatario, mediante un proceso seguro de certificación y verificación, expedido por un prestador de servicios de certificación debidamente acreditado."

Inciso 5: **DATOS DE CREACIÓN DE LA FIRMA**, el concepto utilizado es muy similar al estipulado en el Real Decreto-Ley Español. Por tratarse de un artículo cuyo objetivo es definir, considero que lo relativo a su condición secreta o control exclusivo no debe estipularse dentro de la misma definición.

Inciso 6: **DOCUMENTO ELECTRÓNICO**, así como en algunos casos se abarca mucho en lo relativo a la definición, existen otros casos como este que es impreciso al olvidar mencionar las transacciones las cuales también pueden ser parte de las representaciones electrónicas.

Asimismo, no sólo se puede recuperar o reproducir, es importante mencionar que se puede conservar. El término conservar

debe introducirse en este concepto, debido a que es parte de la función del Sistema Nacional de Archivos el velar con el cuidado y conservación de algunos documentos en particular.

Inciso 7: **DOCUMENTO DIGITAL**, considero que no es necesario incorporar este término a las definiciones, debido a que hace el texto más complicado.

Si revisamos la ley argentina, peruana, venezolana, colombiana, española e incluso la ley modelo de la CNUDMI para las firmas electrónicas, nos damos cuenta que ninguna de estas define el término documento electrónico, mucho menos documento digital.

Inciso 8: **FIRMA DIGITAL**, además de lo estipulado como firma digital, es importante un punto que es omiso en esta definición y se encuentra presente en la ley colombiana la cual dice "(…) permite determinar (…) que el mensaje inicial no ha sido modificado después de efectuada la transformación."[180]

Con este pequeño texto que se le agregue le da a la firma digital, un carácter de integridad e inequivoquidad.

[180] Notaría 19, Bogotá, Congreso de la República, Ley 527 del 1999 (agosto 18), artículo 2 definiciones.

Inciso 10: **INFORMACIÓN INTEGRA**, es preciso agregar en esta definición, después de "inalterada" un texto que diga ".. desde el momento de su emisión."[181]

Si se estipula así, la información puede que sea completa e inalterada desde cierta fecha, no garantizándose la integridad e inalterabilidad del documento desde el momento de su emisión.

Inciso 12: **PRESTADOR DE SERVICIOS DE CERTIFICACIÓN O ENTIDAD CERTIFICADORA**, debemos recordar que los prestadores de servicios de certificación, pueden prestar otros servicios relacionados con la firma digital no sólo certificar.

Es así como vemos, en la Ley modelo de la CNUDMI para las firmas electrónicas, que define a los prestadores de servicios de la siguiente forma: "(…) es la persona física o jurídica que expide certificados, **pudiendo prestar, además, otros servicios en relación con la firma electrónica.**"[182]

Al agregarle lo anterior al texto se le da un matiz más amplio y mayor libertad de competencia a nuestros prestadores de servicios.

---

[181] Este texto es tomado del Proyecto de Ley de Firmas y documentos electrónicos, brindado en el Seminario Impartido en La Universidad Latina de Costa Rica, el día 18 y 19 de junio del 2003, por el MS.c Edwin Aguilar Sánchez.

[182] Estado Español, Real Decreto-Ley 14/1999 del 17 de setiembre, sobre firma electrónica, artículo 2. La negrita no es original del texto.

Asimismo, no debemos confundir los términos de prestador de servicios con entidad certificadora o autoridad de certificación debido a que estas son distintas.

Según los concursantes al Postgrado en E-Business Management Universidad del Salvador (ARGENTINA) - Georgetown University (USA) definen ambos términos de la siguiente forma:

La Autoridad de Certificación "es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actuaría como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información."[183]

Los Servidores de Certificación "son aplicaciones destinadas a crear, firmar y administrar certificados de claves, y que permiten a una empresa u organización constituirse en autoridad de certificación para subvenir sus propias necesidades. Los productos más famosos son Netscape Certificate Server y OpenSoft."[184]

---

[183] Firma y Certificado Digital, Postgrado en E-Business Management Universidad del Salvador (ARGENTINA) - Georgetown University (USA) Catedra Marco legal Año 2001, http://www.hfernandezdelpech.com.ar/Leyes/TRABAJO%20FIRMA%20DIGITAL%20POSTGRADO%20E.-BUSINESS.htm , Pág.10

[184] Firma y Certificado Digital, Postgrado en E-Business Management Universidad del Salvador (ARGENTINA) - Georgetown University (USA) Catedra Marco legal Año 2001, http://www.hfernandezdelpech.com.ar/Leyes/TRABAJO%20FIRMA%20DIGITAL%20POSTGRADO%20E.-BUSINESS.htm , Pág.11

Habiendo aclarado estos términos sería prudente eliminar uno de estos, el cual considero debe de ser el término Prestador de Servicios.

En el último inciso 15 de este artículo segundo, debido a que en la totalidad de este proyecto se utiliza indiferentemente signatario o firmante, considero por lo anterior, que dentro de este inciso se debe agregar a la par de signatario "o firmante".

ARTÍCULO 3.- Este artículo es muy similar al estipulado por la Ley modelo de la CNUDMI para las firmas electrónicas. Si embargo hace referencia a la firma digital acreditada, lo que considero no es necesario determinar, esto debido a que sea acreditada o no debe cumplir los requisitos de esta ley.

ARTÍCULO 5.- Este artículo es de suma importancia debido a que puede llegar a abarcar la labor del notario en lo que respecto a certificación de actos o cualquier otro tipo de documentos.

Entres distintos jurisconsultos alrededor del mundo, discuten lo referente a este tipo de certificación, por considerarla una doble certificación innecesaria.

Esto se debe a que en la práctica la firma digital es acompañada de un certificado que identifica de manera confiable e

inequívoca, que el que firma un documento electrónico es quién dice ser realmente, por lo que muchos creen, no es necesario certificar nuevamente ese hecho.

El problema que yo analizo aquí, es que pasaría si esa firma no es digital sino electrónica, en ese caso creo que debe de certificarse por medio de la firma digital de un funcionario público o cualquier persona autorizada y competente para esos fines.

De igual forma si la firma que se realiza, no posee un certificado acreditado podría el funcionario o cualquier persona autorizada y competente certificar que la firma digital corresponde a quien dice ser, claro está siempre que se compruebe de manera fehaciente la misma.

El artículo no consigna el mensaje de datos, abarcando este concepto según el artículo segundo, múltiples informaciones electrónicas que a raíz de su importancia debería incluirse dentro del mismo.

ARTÍCULO 6.- Las discusiones en la Asamblea Legislativa respecto a lo que estipula este artículo, han ayudado a que este mejore y brinde igualdad de oportunidades a todos.

A pesar de las diversas discusiones en la Asamblea Legislativa, en el artículo se combina la autorización para utilizar la firma digital junto a la autorización para poder actuar como entidades certificadoras, lo cual son puntos que deben ir contemplados por aparte.

El término "(…) en los que sea aplicable…" considero debe cambiarse por "cuando corresponda", para evitar confusiones, debido a que sería siempre o al menos en la mayoría de los casos "aplicable" la Ley del Sistema Nacional de Archivos.

ARTÍCULO 7.- Debe estudiarse y analizarse que es lo que quiere decir el autor del texto, cuando se refiere a "asegurar razonablemente su secreto y seguridad razonable", el significado de razonable puede ser muy distinto entre unos y otros, lo cual crea inseguridad.

El inciso 5, de este artículo está incluido dentro del inciso 2, debido a que si hay alteración, esta se realiza en el documento, transacción o mensaje de datos, no en la firma.

ARTÍCULO 8.- Es prácticamente una copia fiel del artículo 22 del Real Decreto-Ley Español 14/1999 del 17 de setiembre, sobre firma electrónica. Sin embargo, al comparar con otras legislaciones como la

panameña, la colombiana y en especial con la Ley modelo de la CNUDMI, podemos observar que en estas legislaciones que existe ningún apartado especifico que regule lo referente a los dispositivos de verificación de la firma digital.

Por lo que habrá que estudiar y analizar, si realmente es indispensable la regulación en esta ley de dichos dispositivos.

b.- TÍTULO SEGUNDO: DEL ÓRGANO RECTOR Y LA AUTORIDAD ACREDITADORA.

Para los efectos de esta Ley debemos estar claros que el Órgano Rector es el Ministerio de Ciencia y Tecnología, y que la Autoridad Acreditadota, será un órgano subordinado a dicho Ministerio, el cual no se especifica en este texto.

Este título está conformado por los artículos del 10 al 14 que se estipulan en el texto origen de la presente investigación, cuyas observaciones son las siguientes:

ARTÍCULO 11.- Inciso a) Se debe tomar en cuenta que la Autoridad Acreditadota, otorgará licencias, pero también deberá prorrogarlas, cosa que no se encuentra estipulado dentro de este inciso.

Inciso d): Se pueden dar normas de acatamiento e instrucciones que deben llevarse a cabo, pero instrucciones sobre el adecuado cumplimiento no.

Debido a que el cumplimiento adecuado, es voluntad y facultad de las partes, las cuales a su vez serán responsables y hasta sancionadas según corresponda, si no cumplen con lo estipulado. Sería como estar repartiendo consejos para portarse bien y no tener problemas.

Cada persona ya sea física, jurídica, privada o pública tiene que cumplir con las leyes y reglamentos, de lo contrario se atiene a las consecuencias.

Inciso e): Lo que se suspende o revoca es la Licencia no la acreditación.

Otras de las funciones que de acuerdo con el Proyecto de firmas y documentos electrónicos[185], artículo 32 deben de tener son:

- Fijar y proponer las políticas generales en materia de firma electrónica y su desarrollo.

[185] Proyecto de Ley de Firmas y documentos electrónicos, artículo 32, inciso a, d,e, brindado en el Seminario Impartido en La Universidad Latina de Costa Rica, el día 18 y 19 de junio del 2003, por el MS.c Edwin Aguilar Sánchez.

- Velar por la transparencia, oportunidad y legalidad de los actos y procedimientos administrativos.
- Resolver las apelaciones presentadas contra los procedimientos y los resultados finales de registro de las entidades certificantes, así como los procedimientos de sanción.
- Fiscalizar el funcionamiento de las entidades para asegurar su confianza, eficacia y cumplimiento de la normativa aplicable.

ARTÍCULO 12.- Segundo Párrafo, además de las funciones aquí estipuladas, sería bueno consultar lo que estipula el Parlamento Europeo y El Consejo de la Unión Europea, que en lo conducente dice:

"Los proveedores de servicios de certificación deberán:

a) demostrar la fiabilidad necesaria para prestar servicios de certificación;

b) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

c) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

d) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;

e) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas;

f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

g) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos;

h) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular

para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado;

i) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

j) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves;

k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información

estarán también disponibles a instancias de terceros afectados por el certificado;

l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

— sólo personas autorizadas puedan hacer anotaciones y modificaciones,

— pueda comprobarse la autenticidad de la información,

— los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y

— el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados."[186]

Aunque la mayoría de estas son obligaciones de los prestadores de certificación, o como se le menciona en el proyecto entidades de certificación, las mismas figuran un papel importante en la regulación y establecimiento de los derechos y obligaciones de las partes que participen en la utilización de la firma digital, lo anterior debe de tomarse en cuenta en el reglamento.

[186] Directiva 1999/93/CE del Parlamento Europeo y del Consejo de la Unión Europea de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, Anexo II, Pág. 19.

ARTÍCULO 14.- Se menciona nuevamente al Ministerio de Ciencia y Tecnología, a los Prestadores de Servicios y a la Autoridad de Acreditación, considero que esta mención es ambigua e innecesaria.

Con el sólo hecho de que en el segundo párrafo después de Autoridad de Acreditación se agregue "junto al Ministerio de Ciencia y Tecnología", es posible eliminar el primer párrafo y evitar confusiones y problemas a futuro.

c.- TÍTULO TERCERO: DE LOS CERTIFICADOS DIGITALES.

ARTÍCULO 15.- Los certificados digitales se vinculan con una persona, no debe cometerse en nuestra legislación los errores cometidos en otras legislaciones.

Tal y como señala el jurisconsulto Diego García de las Heras en "La Persona Jurídica como Signatario de una Firma Electrónica"[187], la firma digital regulada en el Real-Decreto ley español, peca de no

[187] La Persona Jurídica como Signatario de una Firma Electrónica, Autor: Diego García de las Heras, Especialistas Derecho Nuevas Tecnologías, ghdiego@yahoo.es, Última actualización 15 de Abril 2002, www.Portaley.com

incluir la titularidad de la persona jurídica en el desarrollo y aplicación de la firma digital.

Error que nosotros al crear nuestra normativa, no debemos cometer, por lo que este artículo no sólo debe vincularse con una persona, por el contrario debe estipularse que dicho vínculo es independiente, de si se trata de una persona física o jurídica, quién podrá estar vinculada con el o los certificados digitales.

ARTÍCULO 17.- Dentro de estas circunstancias para suspender, cancelar y revocar debemos adicionar otros puntos:

En el inciso 3, después de "cese" debería de adicionarse, "quiebra o liquidación", y al final de este inciso agregar la figura del usuario, el cual puede verse afectado por estas condiciones.[188]

[188] En referencia a este punto podemos ver la Ley Panameña, Ley No. 431 De 31 de julio de 2001,Que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos; Artículo 33. Causales para la revocación de certificados (…) Una entidad de certificación revocará un certificado emitido por las siguientes razones: a. Petición del suscriptor o un tercero en su nombre y representación, **b. Muerte del suscriptor, c. disolución del suscriptor**, en el caso de las personas jurídicas, d. Confirmación de que alguna información o hecho, contenido en el certificado, es falso, e. La privacidad de su sistema de seguridad ha sido comprometida de manera material, que afecte la confiabilidad del certificado, f. Cese de actividades de la entidad de certificación(…) Paralela a esta podemos ver como la Ley colombiana y Guatemalteca incluyen los aspectos aquí recomendados, respectivamente son los siguientes: Ley 527 de 1999, Artículo 37. Revocación de certificados (…) Una entidad de certificación revocará un certificado emitido por las siguientes razones:1. A petición del suscriptor o un tercero en su nombre y representación, 2. Por muerte del suscriptor, 3. Por liquidación del suscriptor en el caso de las personas jurídicas (…) y Ley para la Promoción del Comercio Electrónico y Protección de la Firma Digital, Artículo 41. Revocación de certificados (…) Una sociedad de certificación revocará un certificado

Asimismo, podemos agregar a este artículo dos incisos más. Como punto octavo podemos incluir a pesar de estar regulado dentro de nuestra normativa general: El incumplimiento de pago y como punto noveno la posible suspensión y hasta revocación por sospechas fundadas de su confiabilidad y seguridad que también es regulado en las leyes guatemaltecas, colombiana y panameña.

Es conveniente al llegar a este punto, hacer énfasis a las distintas características que posee un certificado en algunas legislaciones, no tan mencionadas en la presente investigación.

Considero importante visualizar y tener presente el cuadro confeccionado por los concursantes del Postgrado en E-Business Management Universidad del Salvador (ARGENTINA) - Georgetown University (USA), en este cuatro se toma en cuenta la legislación peruana, chilena y el Real Decreto-Ley.

Puntualiza diversos aspectos tales como las definiciones de certificados dadas en cada país, los requisitos de validez, la confidencialidad, la extinción o cancelación y los certificados extranjeros.

---

emitido por las razones siguientes: 1. A petición del suscriptor o un tercero en su nombre y representación, 2. Por muerte del suscriptor, 3. Por liquidación del suscriptor en el caso de las personas jurídicas (...).La negrita no corresponde la texto original se ha resaltado con fines de visualización y análisis del articulado del proyecto 14276.

CERTIFICADO DIGITAL.[189]

Generales	**Ley Peruana**	**Proyecto Ley Chilena**	**Real Decreto-Ley**
Definición	Documento electrónico generado y firmado digitalmente por entidad de certificación y vincula par de claves con persona confirmando su identidad.	Certificación electrónica que da fe sobre los datos referidos a firma electrónica simple o avanzada.	Denominado *certificado electrónico*, es la certificación electrónica que vincula datos de verificación de firma a un signatario y confirma su identidad.
Contenido/ requisitos	1. Datos suscriptor 2. Datos Entidad de Certificación 3. Clave publica 4. Metodología verificación 5. Número de serie certificado 6. Vigencia 7 Firma Digital de Entidad de Certificación	1. Identificador de Autoridad de Certificación 2. Nombre del titular con su Rol Único Tributario 3. Dispositivo de verificación de firma 4. Periodo de validez 5. Código identificativo único del Certificado 6. FE de Autoridad de Certificación 7. Límites uso del Certificado 8. Un atributo específico del titular (ej. Dirección)	Como subespecie a la que se refiere el Real decreto- ley se encuentra el certificado electrónico reconocido, que es aquél que: a) contiene: • la identificación de que se expiden como tal • identificador del prestador de servicio de certificación (nombre, razón social, domicilio, número de identificación fiscal, etc.) • firma electrónica avanzada del prestador de servicios • identificación del signatario por su nombre y apellidos o a través de un pseudónimo inequívoco • la indicación en el documento que acredite la facultad del signatario de actuar por sí o en nombre de otra persona física o jurídica • los datos de verificación de la

[189] Cuadro Comparativo de Firma y Certificado Digital, Postgrado en E-Business Management Universidad del Salvador (ARGENTINA) - Georgetown University (USA) Catedra Marco legal Año 2001, http://www.hfernandezdelpech.com.ar/Leyes/TRABAJO%20FIRMA%20DIGITAL%20POSTGRADO%20E.-BUSINESS.htm , Pág.17. Vemos como este cuadro hace referencia a lo mencionado en la nota de pie anterior a esta, que es lo referente a la revocación.

			firma que correspondan a los datos de creación de la misma y que se encuentren bajo el control del signatario • el comienzo y el fin del período de validez del certificado • sus límites de uso • si existen límites en el valor de las transacciones para las que puede utilizarse el certificado b) es expedido por un prestador de servicios de certificación que cumple determinados requisitos.
Confidencialidad	Entidad Certificante recaba datos directos del solicitante. Solo puede revelar clave privada por orden judicial o pedido del suscriptor.		
Extinción		Por expiración plazo convencional o máximo legal de 3 anos.	El plazo de validez está definido en el mismo certificado y sus plazos de validez regulados por la entidad de registro.
Cancelación	1. Solicitud del titular 2. Revocación de E.C. 3. Expiración plazo 4. Cese de operaciones del E.C.	Generalmente como sanción: se elimina la inscripción del prestador en el registro de prestadores acreditados.	
Revocación	* Información certificado inexacta o ha sido modificada * Muerte del titular * Incumplimiento relación contractual	* Solicitud del suscriptor * Muerte del titular/ disolución entidad jurídica * Resolución judicial, quiebra.	
Certificado digital extranjero	Misma validez y eficacia jurídica de Ley peruana solo si reconocido por entidad de certificación nacional del país de origen		No prevee restricciones para los estados miembros de la Unión Europea (sin referencia a otros países)

d.- TÍTULO CUARTO: DEBERES DE LAS PARTES INTERVINIENTES.

ARTÍCULO 19.- Este artículo en su totalidad es confuso y sumamente subjetivo. Vemos que se usan términos como razonable, dilatación indebida, riesgo considerable, ciclo vital entredicho, entre otros.

El uso de estos términos puede desvirtuar el fin y la intención que tenía el jurista al confeccionar la ley, dando muletillas y obstáculos para que se pueda interpretar la ley dependiendo de quién la tenga en sus manos.

El Master Edwin Aguilar en su seminario sobre el Proyecto de Ley de Firmas y documentos electrónicos, hace entrega de un texto muy diferente al proyecto presentado en la Asamblea Legislativa del cual podemos salvar del texto entregado, un artículo que podría consignarse en lugar del que se encuentra en discusión en este momento.

No obstante, en este artículo se hace referencia a un sistema, el cual no se describe en el texto por lo que considero es mejor eliminar dentro del texto dicha palabra.

El artículo es el numeral catorce y se divide en tres puntos:

"Artículo 14.- **Obligaciones y responsabilidades**

Los (las) usuarios(as) del sistema de firma electrónica estarán obligados(as) a:

a) Suministrar a las entidades certificantes la información veraz, completa y actualizada que requieran para la prestación de sus servicios.

b) Resguardar estrictamente la confidencialidad de la clave, contraseña o mecanismo de identificación similar que se les haya asignado, informando inmediatamente a la entidad certificante en caso de que dicha confidencialidad se vea o se sospeche que ha sido comprometida.

c) Acatar las recomendaciones técnicas y de seguridad que le señale la correspondiente entidad certificante.

Sin perjuicio de la eventual responsabilidad penal que corresponda, los (las) usuarios(as) particulares del sistema serán civilmente responsables por todos los daños o perjuicios que deriven del incumplimiento de sus obligaciones, siempre que medie dolo o culpa.

La Administración y sus agentes responderán de acuerdo con lo dispuesto en la Ley General de la Administración Pública y demás legislación aplicable."[190]

ARTÍCULO 20.- Nuevamente, se hace referencia a los términos razonables, importantes, ciclo vital entre otros; que se mencionó en el análisis del artículo anterior, lo cual acarrea confusión.

En el punto dos, de este artículo se hace referencia a las declaraciones las cuales según el artículo tienen que ser exactas y completas, sin embargo considero que el legislador omitió estipular que además deben de ser verdaderas.

En el punto tres, inciso c), dice: "Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella". De conformidad con el desarrollo de la presente investigación, hemos mencionado en un sin numero de ocasiones, que la firma es confiable, en casi un 99.9%, cuando este respaldada por un certificado, no antes de esto.

[190]Proyecto de Ley de Firmas y documentos electrónicos, artículo 14, brindado en el Seminario Impartido en La Universidad Latina de Costa Rica, el día 18 y 19 de junio del 2003, por el MS.c Edwin Aguilar Sánchez.

Es así como los datos de creación de la firma serán validos desde la fecha en que se emitió el certificado, no antes de esto.

ARTÍCULO 21.- Es importante, evitar confusiones al utilizar el término de firma electrónica y firma digital debido a que son muy diferentes.

En este artículo en el Inciso uno, se hace referencia a la firma electrónica y no a la firma digital como se había venido denominando, por lo que considero que este término debe corregirse.

J. Andrés Hall y Mauricio Devoto manifiestan que: "…corresponde hablar de firma digital y no de firma electrónica, vocablo este último que se utiliza erróneamente en cierta legislación internacional para referirse a la firma mecanizada para los fines de su procesamiento informático, la que consiste más precisamente de dígitos (binarios) que de electrones."[191]

ARTÍCULO 22.- Este en general está bien, sin embargo debe analizarse el orden gramatical en el cual se han redactado las oraciones, debido a que en muchos casos es reiterativo y redundante.

[191] J. Andrés Hall y Mauricio Devoto, en su libro La Firma Digital: Herramienta Habilitante del Comercio Electrónico, Pág. 27

Asimismo, el término activo viene de patrimonio y significa: "el haber total de una persona natural y jurídica (…) importe en general valores efectivos, créditos y derechos que el comerciante tiene a su favor. En el activo figura todo lo que posee o cabe acreditar."[192]

Por lo que cabe analizar si realmente el legislador busca aplicar esta palabra en el inciso a), o si por el contrario, busca la aplicación como en las demás legislaciones de una garantía, que respalde las actuaciones de los prestadores de servicios de certificación.

e.- TÍTULO QUINTO: SANCIONES.

El término sanción se entiende como: "La amenaza legal de un mal por la comisión u omisión de ciertos actos o por la infracción de determinados preceptos (…) Pena para un delito o falta(…)"[193]

Ahora habiendo definido el concepto de sanción podemos entrar al análisis del capítulo quinto del proyecto 14.276.

ARTÍCULO 23.- Nuevamente debemos revisar la ortografía y orden gramatical del artículo. Debido a que se dejan palabras

[192] Diccionario Jurídico Elemental, Guillermo Cabanellas, Edición 1998, Editorial Heliasta.

[193] Diccionario Jurídico Elemental, Guillermo Cabanellas, Edición 1998, Editorial Heliasta.

incompletas en el texto, ejemplo de esto es que en el segundo párrafo de este artículo en lugar de "no" se pone solamente "n".

Asimismo, en el primer párrafo de este artículo dice: "Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que, **en el perjuicio** de su actividad ocasionen por la certificación u homologación de certificados de firmas digitales. (…)"[194]

La palabra subraya, "en perjuicio" no corresponde al sentido del artículo. Considero que en lugar de está, el legislador buscaba interpretar que los prestadores de servicios de certificación, serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen.

ARTÍCULO 24.- De nuevo es reiterativo, ejemplo de esto es que en el inciso d), se repite dos veces y de forma continua "de entidad".

Si lo que se pretende es crear un reglamento para esta ley, no podemos olvidar y por el contrario debemos facultar al reglamento para que pueda crear otras sanciones.

Es así como debe agregarse a este artículo un inciso f) que diga: "Las demás que el Reglamento de esta ley establezca", logrando

[194] Asamblea Legislativa, Asuntos Jurídicos "Proyecto de Ley 14.276", Texto Sustitutivo, folio 591.

generalizar y abrir las puertas a una mayor y mejor regulación de esta figura tan importante como lo es la firma digital.

En el inciso a) de este artículo se habla de amonestación por escrito, sin embargo no define que es lo que ocurre si se amonesta, ¿Corresponderá a una multa? o si la reiteración de un número de amonestaciones equivalen a algo en específico.

A pesar de que como hemos ido analizando el proyecto se ha mejorado, todavía faltan temas y puntos que se deben de incluir dentro del texto.

Algunos de los puntos importantes que se mencionan brevemente en el texto o no se mencionan del todo son:

1. La forma, gestión y conservación de los documentos electrónicos, mensajes electrónicos o algún archivo digital.
2. En caso de que las partes sean omisas o no sean claras, en estipular cual ley van a aplicar, se estipule la de nuestro país.
3. Falta estipular sobre las obligaciones de indemnizar a la o las partes afectadas.

4. Se debe estipular de una mejor forma, la calificación de fuerza probatoria que posee la firma digital.
5. Para evitar futuros problemas, y por la misma naturaleza de la firma digital que puede utilizarse en cualquier parte del mundo, se debe estipular un domicilio electrónico.

Entiendase por domicilio electrónico, el lugar donde puedan las partes recibir notificaciones, en este caso se trata de una dirección electrónica a la cual remitir las notificaciones o comunicaciones.

SECCIÓN TERCERA: PROPUESTA DE TEXTO SUSTITUTIVO.

Después del desarrollo de la presente investigación, y con la ayuda de la doctrina comparada, se ha diseñado una propuesta de texto sustitutivo.

La siguiente propuesta que me he atrevido a diseñar, se ha realizado tomando como base el último texto sustitutivo presentado por los señores Solano Solano y Acosta Polonio, que fue aprobado por la Asamblea Legislativa y se encuentra en discusión.

LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1.- La presente Ley tiene por objeto reconocer y regular el uso de la Firma Digital y los Certificados Digitales, otorgándole a los documentos firmados digitalmente la misma validez y eficacia jurídica que aquellos con firma manuscrita que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización.

No obstante, no se aplicará la firma digital y certificados digitales en los siguientes casos:

a) En las obligaciones contraídas por el Estado en virtud de Convenios o Tratados Internacionales.

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

ARTÍCULO 2.- Para los propósitos de la presente Ley se establecen las siguientes definiciones:

1. **Acreditación:** Es el procedimiento mediante el cual la Autoridad de Acreditación, creada en esta ley, reconoce formalmente que una persona física, jurídica, pública y privada es competente para realizar las tareas de certificación digital, de acuerdo a las normas nacionales e internacionales.
2. **Acreditación de la entidad de certificación:** Procedimiento que establece los derechos y obligaciones específicos para la entidad de certificación y que se emite, a petición del interesado, por la Autoridad de Acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa internacional aplicable.

3. **Certificado Digital:** todo mensaje de datos u otro registro que confirme un vínculo entre un firmante y los datos de creación de la firma digital.
4. **Certificado Digital Reconocido:** es el certificado digital que cumple con los requisitos establecidos en la presente ley y su reglamento, vinculando una firma digital con su signatario, mediante un proceso seguro de certificación y verificación, expedido por una entidad de certificación debidamente acreditado
5. **Datos de creación de firma:** Son los datos únicos, como códigos, atributos biométricos o claves criptográficas privadas, que el signatario utiliza para crear su Firma Digital. Estos datos quedan en entredicho si se ha perdido su confidencialidad o control exclusivo por parte del signatario.
6. **Documento electrónico:** es toda la representación electrónica de actos, transacciones, hechos, datos o descripciones, y que se puede recuperar, reproducir o conservar en forma perceptible e inteligible.
7. **Firma Digital:** Es el conjunto de datos asociados funcionalmente a un documento electrónico, utilizados como medio para

identificar formalmente al firmante e indicar que este aprueba el contenido de este documento. Asimismo permite determinar que el mensaje inicial no ha sido modificado después de efectuada la transformación.

8. **Firma Digital Acreditada:** Es la firma digital certificada por una entidad de certificación debidamente acreditado ante la Autoridad de Acreditación.
9. **Información Interna:** aquella información que haya permanecido completa e inalterada desde el momento de su emisión, sin menoscabo de cualquier adición o cambio accesorio, inherente al proceso de comunicación, almacenamiento, archivo o presentación.
10. **Mensaje de Datos:** Es la información generada, enviada, recibida, almacenada o comunicada por medios digitales, electrónicos, ópticos o similares.
11. **Entidad certificadora:** Es la persona física o jurídica que expide certificados, pudiendo prestar además, otros servicios en relación con la firma digital.
12. **Dispositivo o Procedimiento de verificación:** Es el proceso empleado con el propósito de verificar que una Firma Digital es

atribuible a determinada persona como su signatario, o para detectar cambios y errores en un documento digital.

13. **Parte que confía:** persona que puede actuar sobre la base de un certificado o de una firma digital.
14. **Signatario o firmante**: Es la persona física o jurídica que cuenta con un mecanismo de creación de firma, que actúa en nombre propio o con poderes de representación de otra persona física o jurídica.

ARTICULO 3.- Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria de conformidad con la legislación nacional vigente. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

ARTICULO 4.- Ninguna de las disposiciones de la presente Ley, será aplicada de modo que excluya, restrinja o prive de valor y efecto jurídico cualquier método para crear, de forma segura una firma digital, que cumpa los requisitos de la Ley.

ARTICULO 5.- El documento o mensaje de datos firmado digitalmente que hay sido producido por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados el mismo valor y eficacia jurídico que la firma manuscrita en relación con los datos consignados en papel.

Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento digital si el mismo ha sido firmado mediante una Firma Digital Acreditada.

Se presumirá que la Firma Digital y el medio de creación de la firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en esta Ley cuando el certificado digital reconocido es emitido por una entidad certificadora acreditado ante la Autoridad de Acreditación.

ARTICULO 6.- Cuando una ley requiere que un documento, mensaje de datos o firma esté certificado o de cualquier otra forma reconocida, verificado tal requisito se tendrá por cumplido si una firma digital acreditada de un funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento firmado.

ARTICULO 7.- Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, así como todas las instituciones públicas descentralizadas, y entes públicos no estatales y cualquier dependencia del sector público, incluso en las estructuras según modelos organizacionales del Derecho Privado para la utilización de la firma digital acreditada en los documentos electrónicos en sus relaciones internas, entre ellos y con las particulares. Así como para poder actuar como entidades certificadoras, siempre que cumplan todos los requisitos que para este efecto se establezcan, de conformidad con las previsiones de esta Ley y su reglamento. En lo atinente a los documentos electrónicos firmados digitalmente se deberá cumplir cuando corresponda con lo que establece la Ley 7202, Ley del Sistema Nacional de Archivos.

ARTICULO 8.- Los dispositivos seguros de creación de Firma Digital para considerarse como tales deberán cumplir con lo siguiente:

1. Garantizar que los datos utilizados para la generación de la firma puedan producirse sólo una vez y que corresponden exclusivamente al firmante, asegurando su secreto, dentro de las posibilidades o limitaciones tecnológicas.

2. Brindar seguridad de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado y que es posible detectar cualquier alteración en el mensaje de datos con posterioridad al momento de firmar.
3. Proteger los datos de creación de firma por el signatario contra la utilización por otros y que en el momento de firmar están bajo su control.
4. Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

ARTÍCULO 9.- Los dispositivos de verificación de Firma Digital Acreditada deben de garantizar al menos lo siguiente:

1. Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.
2. Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.
3. Que aparezca correctamente la identidad del signatario.
4. Que se verifique de forma fiable el certificado.

5. Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.
6. Los demás que el reglamento establezca.

ARTICULO 10.- Las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte.

ARTICULO 11.- Tanto en transacciones privadas como en las realizadas con o por el Estado, las personas físicas o jurídicas deberán señalar una dirección de correo electrónico como su domicilio para la recepción de cualquier clase de comunicaciones, respecto del acto o contrato realizado.

CAPÍTULO II

DEL ÓRGANO RECTOR Y LA AUTORIDAD ACREDITADORA

ARTICULO 12.- El Ministerio de Ciencia y Tecnología será el Órgano Rector en todo lo concerniente a esta Ley.

Toda interpretación técnica estará bajo el mejor criterio del Órgano Rector tomando ene cuenta los avances tecnológicos, así como los requerimientos y realidades del país.

ARTÍCULO 13.- Créase la Autoridad Acreditadora como órgano subordinado al Ministerio de Ciencia Y Tecnología y entre sus funciones estarán:

a) Autorizar la actividad de las entidades de certificación en el territorio nacional otorgando y prorrogando licencias de operación.
b) Fiscalizar el funcionamiento y la eficiente prestación del servicio por parte de las Entidades de Certificación.
c) Imponer sanciones a las Entidades de Certificación en caso de incumplimiento de las obligaciones derivadas de la prestación de servicio.
d) Impartir instrucciones de las normas a las cuales deben sujetarse las Entidades de Certificación.
e) Revocar o suspender la licencia otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en la presente Ley.

f) Mantener, procesar, clasificar, resguardar y custodiar el Registro de las Entidades de Certificación de acuerdo a lo dispuesto en los reglamentos respectivos.

g) Recaudar multas de acuerdo a lo dispuesto en los reglamentos respectivos.

h) Actuar como conciliador en la solución de conflictos que se susciten entre las Entidades de Certificación y sus usuarios, cuando ello sea solicitado por al menos una de las partes involucradas, sin que renuncie al trámite de jurisdicción ordinaria o a las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a esta ley y los reglamentos respectivos.

i) Fijar y proponer las políticas generales en materia de firma digital y su desarrollo.

j) Velar por la transparencia, oportunidad y legalidad de los actos y procedimientos administrativos.

k) Resolver las apelaciones presentadas contra los procedimientos y los resultados finales de registro de las

entidades certificantes, así como los procedimientos de sanción.

l) Fiscalizar el funcionamiento de las entidades para asegurar su confianza, eficacia y cumplimiento de la normativa aplicable

m) La demás que le asigne el reglamento.

ARTÍCULO 14.- Mediante la Autoridad de Acreditación, las empresas que emitan certificados de firma digital deberán someterse al proceso de acreditación que se defina en el reglamento.

Serán funciones de las empresas certificadoras las de emitir, suspender, cancelar o revocar certificados digitales así como brindar otros servicios inherentes al propio certificado.

ARTÍCULO 15.- La Autoridad de Acreditación así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y la custodia de los documentos y la información que le entreguen las empresas certificadoras.

ARTICULO 16.- La Autoridad de Acreditación junto al Ministerio de Ciencia y Tecnología, reconocerá formalmente que una organización es competente para llevar a cabo tareas especificas de certificación digital, de acuerdo con los requisitos de normas nacionales e

internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente los derechos de los usuarios.

Para ello deberá llevar a cabo el proceso de evaluación correspondiente, llevar un registro de las entidades acreditadas y velar por que se cumplan los requisitos establecidos por esta Ley y su reglamento mediante prácticas de supervisión y auditorias que acuerden efectuar.

CAPÍTULO III

DE LOS CERTIFICADOS DIGITALES

ARTÍCULO 17.- Los certificados digitales se vínculan con una persona física o jurídica, confirmando su identidad, los cuales deberán contener al menos:

1. Los datos que identifiquen individualmente al firmante.
2. Las normas y procedimientos utilizados para la creación de la firma.
3. Los datos que identifiquen a la entidad de certificación.
4. Número de serie del certificado.
5. Fecha de emisión y plazo de vigencia.

6. Los demás que el reglamento establezca.

ARTÍCULO 18.- Los certificados digitales se suscriben mediante un contrato de servicios de certificación digital entre el suscriptor, que será el titular de la firma, y la entidad de certificación digital acreditada ante la Autoridad de Acreditación.

ARTÍCULO 19.- Los certificados digitales se podrán suspender, cancelar y revocar según sea el caso, en las siguientes circunstancias:

1. A solicitud del titular de la firma.
2. Por vencimiento del plazo de vigencia del certificado.
3. Por cese, quiebra o liquidación de operaciones de la entidad de certificación o del usuario.
4. Por muerte del titular de la Firma Digital.
5. Por incumplimiento contractual con la entidad de certificación.
6. Por orden de un juez.
7. Por incumplimiento de pago.
8. Cuando existan sospechas fundadas de su confiabilidad y seguridad.
9. Las demás que el reglamento establezca.

ARTICULO 20.- Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por las entidades establecidas y acreditadas en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y reconocidos por la autoridad de acreditación competente cumpliendo con los requisitos fijados en esta Ley, y su reglamento y normas internacionales correspondientes.

ARTÍCULO 21.- Los (las) usuarios(as) de la firma digital estarán obligados(as) a:

d) Suministrar a las entidades certificantes la información veraz, completa y actualizada que requieran para la prestación de sus servicios.

e) Resguardar estrictamente la confidencialidad de la clave, contraseña o mecanismo de identificación similar que se les haya asignado, informando inmediatamente a la entidad certificante en caso de que dicha confidencialidad se vea o se sospeche que ha sido comprometida.

f) Acatar las recomendaciones técnicas y de seguridad que le señale la correspondiente entidad certificante.

Sin perjuicio de la eventual responsabilidad penal que corresponda, los (las) usuarios(as) particulares del sistema serán civilmente responsables por todos los daños o perjuicios que deriven del incumplimiento de sus obligaciones, siempre que medie dolo o culpa.

La Administración y sus agentes responderán de acuerdo con lo dispuesto en la Ley General de la Administración Pública y demás legislación aplicable.

ARTICULO 22.- La entidad de certificación, que preste servicios para apoyar una firma digital que pueda utilizarse con efectos jurídicos, deberá:

1. Actuar de conformidad con las declaraciones que hizo ante la Autoridad de Acreditación respecto de sus normas, políticas y prácticas;
2. Actuar con diligencia para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado que emite o que estén consignadas en él, son exactas, verdaderas y complejas;

3. Proporcionar a la parte que confía en el certificado medios accesibles que permitan a ésta determinar mediante el certificado:
    a) La identidad de la Entidad de certificación.
    b) Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;
    c) Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado;
4. Proporcionar a la parte que confía en el certificado medios accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:
    a) El método y procedimiento utilizado para comprobar la identidad del firmante;
    b) Cualquier limitación respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;
    c) Si los datos de creación de la firma son válidos y no están en entredicho;

d) Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho; en caso afirmativo, la entidad de certificación debe efectivamente proporcionar por ese medio al firmante para que de aviso;

e) Si se ofrece un servicio para revocar oportunamente el certificado; en caso afirmativo, la entidad de certificación debe cerciorarse de que existe un servicio efectivo para revocar oportunamente el certificado;

5. Al prestar sus servicios, utilizar sistemas, procedimientos y recursos humanos fiables.

ARTÍCULO 23.-Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

1. Verificar la fiabilidad de la firma digital;
2. Verificar la validez, suspensión o revocación del certificado;
3. Tener en cuenta cualquier limitación explicita en el certificado.

ARTÍCULO 24.- Para determinar si los sistemas, procedimientos o recursos humanos utilizados por una entidad de certificación son fiables y en qué medida lo son, podrán tenerse en cuenta los siguientes factores:

a) Los recursos humanos y financieros, incluida la existencia de una garantía o póliza;
b) La calidad de los sistemas de equipo y programas informáticos;
c) Los procedimientos para la tramitación del certificado, las solicitudes de certificados, y la conservación de registros;
d) La disponibilidad de información para los firmantes nombrados en el Certificado y para las partes que confíen es éste;
e) La periodicidad y el alcance de la auditoría por un órgano independiente;
f) La existencia de una declaración del Estado, de un órgano de acreditación o de la entidad de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y

g) Cualesquiera otros factores pertinentes.

CAPÍTULO V

SANCIONES

ARTICULO 25.- Las entidades de certificación serán responsables de daños y perjuicios, que en su actividad ocasionen por la certificación u homologación de certificados de firmas digitales. En todo caso corresponderá a la entidad de certificación demostrar que actúo con la debida diligencia.

Sin perjuicio de lo anterior, la entidad de certificación no será responsable de los daños o perjuicios que tengan su origen en el uso indebido o fraudulento de un certificado de firma digital por parte del suscriptor.

ARTICULO 26.- Para los efectos de la presente ley se consideran infracciones por parte de las entidades de certificación, el incumplimiento de cualquiera de las disposiciones contenidas en esta ley y la negligencia en la prestación del servicio.

ARTICULO 27.- La Autoridad de Acreditación, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, según la naturaleza y la gravedad de la falta las siguientes sanciones a las

entidades de certificación que incumplan o violen las normas contenidas en la presente ley:

a) Amonestación por escrito, más de tres amonestaciones se aplicará lo estipulado en el inciso b)
b) Multa de cinco hasta veinte salarios base, de acuerdo con el artículo 2 de la Ley 7333.
c) Suspensión inmediata de todas o algunas de las actividades de la entidad infractora.
d) Prohibición a la entidad infractora de prestar directa o indirectamente los servicios de entidad certificación por el término de hasta 5 años.
e) Revocación definitiva de la acreditación y prohibición para operar en Costa Rica como entidad de certificación acreditada.
f) Las demás que el Reglamento establezca.

ARTICULO 28.- Las resoluciones de la Autoridad de Acreditación podrán ser impugnadas por los interesados cuando consideren que han sido perjudicados en sus intereses legítimos o en sus derechos.

Contra dichas resoluciones podrá ser interpuesto el recurso de reconsideración contra la propia Autoridad de Acreditación o apelación ante el Titular del Ministerio de Ciencia y Tecnología.

La Autoridad de Acreditación contará con un plazo de dos meses para decidir sobre le recurso de reconsideración interpuesto. Si en tal plazo no ha sido resuelto el recurso, la decisión se considerará favorable al recurrente.

De la misma forma, el Ministro de Ciencia y Tecnología dispondrá de dos meses para resolver el recurso de apelación. Si en tal plazo este recurso no ha sido resuelto la decisión se considerará favorable al recurrente.

CAPÍTULO VI

DISPOSICIONES FINALES

ARTÍCULO 29.- El Poder Ejecutivo deberá emitir el reglamento a la presente Ley dentro del plazo máximo de tres meses siguientes a su publicación.

La anterior propuesta surge con la idea de poder ayudar a desarrollar una mejor ley que favorezca al pueblo costarricense. La cual debe velar por el desarrollo económico, social y sociocultural de nuestro pequeño país.

No obstaste, es sólo una propuesta que no denota la postura de ninguna autoridad o persona, es entendida exclusivamente a título personal.

CONCLUSIONES

La evolución de la tecnología en los últimos años, sobre todo en el terreno electrónico y digital, ha realizado una enorme transformación en la operatividad de la industria, del comercio, del sector servicios, de los profesionales, e incluso a nivel doméstico.

Asimismo, en la actualidad son muchos los hogares que se encuentran conectados a la red por las múltiples ventajas que conlleva su utilización, dado que permite realizar desde operaciones bancarias o financieras hasta encargar la adquisición de todo tipo de productos.

Los principios fundamentales en los cuales se debe inspirar nuestra legislación a la hora de regular la firma digital son: libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia de la firma digital a la firma manuscrita.

1. Mantener y establecer la libre competencia en todos los servicios relacionados con las firmas digitales o electrónicas.
2. Neutralidad tecnológica: la no discriminación entre distintas tecnologías y, como resultado de esto producir normas que regulen los diversos entornos tecnológicos. Existiendo flexibilidad en las normas a la hora de legislar sobre una determinada figura.
3. Compatibilidad internacional: creando normas uniformes que se puedan adecuar y utilizar tanto a nivel nacional como internacional. Recordemos que por la misma naturaleza de esta figura y debido a que su inserción es en el mercado global, se hace necesario que se legisle de una forma uniforme y compatible con el resto de las leyes y doctrinas internacionales.
4. Equivalencia de la firma digital a la firma manuscrita: la firma respecto de los datos consignados en forma electrónica, tiene los mismos efectos jurídicos que la firma manuscrita con relación a los datos consignados en papel.

La firma es una forma de exteriorización de la voluntad humana. La voluntad puede manifestarse por diferentes formas, por un gesto, palabras, escritura, fax, etc. Es por esto que la ley debe reconocer una

forma electrónica valida y eficaz de consentir los documentos electrónicos.

La doctrina jurídica conviene en que la firma es el género, la firma electrónica una especie y dentro de ésta encontramos subespecies, tales como las denominadas en algunas legislaciones como firma digital, firma electrónica avanzada, ó firma electrónica certificada.

La firma es la prueba de la manifestación de la voluntad que permita imputar la autoría e identificar al firmante de un documento.

La firma electrónica es un método o símbolo basado en medios electrónicos utilizado o adoptado por una persona con la intención de vincularse o autenticar un documento.

La firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para Firmar un documento digital, su autor utiliza su propia clave secreta (sistema Criptográfico asimétrica), a la que solo tiene acceso, lo que impide que pueda después negar su autoría (no-revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma.

El documento privado es todo escrito que da constancia de un hecho u acto con consecuencias jurídicas, que ha sido firmado por particulares sin intervención de un funcionario público competente, por lo que no tiene otro requisito más que estampar la firma. Es así como un documento electrónico no podría considerarse un instrumento privado mientras no se establezca una ley que regule y de efectos jurídicos de firma digital.

Por lo tanto, la eficacia jurídica del documento electrónico viene condicionada por la necesidad de regulación de la firma digital con la cual se otorgaría un valor probatorio.

Es por ello que considero necesario y adecuado brindar un marco legal dentro del cual pueda desarrollarse y aplicarse la figura de firma digital, creando mayor seguridad jurídica para determinado tipo de actos. No obstante debe tenerse cuidado al aprobar una ley como está, debido al tecnicismo que muchas veces presenta, siendo necesaria la ayuda de técnicos en la materia no sólo en derecho sino en informática.

Es definitivamente un reto bastante grande para el Derecho, la regulación de las tecnologías informáticas, la implementación de un sistema normativo que sea capaz de hacer frente a estos avances, de

manera que generemos una mayor apertura socioeconómica tanto a nivel nacional como internacional.

Precisamente la finalidad de esta investigación, se encuentra en denunciar y especificar una serie de lineamientos sobre la necesidad de que exista una normativa que se adecue a la realidad costarricense, brindando seguridad y eficacia a la hora de utilizar herramientas como el Internet.

Las principales conclusiones de la problemática que hemos planteado durante esta investigación son las siguientes:

a.- Existe una tendencia general hacia el aumento de cantidad de personas, páginas de web, etc. en Internet. Desde su creación hasta la fecha la red ha mostrado tener una aceptación mundial, logrando una apertura del comercio de ahí su importancia de un aumento más significativo.

b.- Es imposible negar el impacto que ha producido la informática en el derecho y sobre todo en el derecho comercial. La posibilidad de realizar maniobras desde lugares lejanos que puedan producir derechos y obligaciones es algo sumamente novedoso.

c.- Debe diferenciarse a la hora de desarrollar "Los Nuevos Estilos de Firma", diversos conceptos básicos tales como los que

corresponden a "Firma Electrónica" y "Firma Digital". En esta investigación se ha analizado ambos tipos, debido a la confusión que se realiza en distintas doctrinas de diversos países.

d.- Nuestro ordenamiento podría verse reformado durante este Gobierno. Actualmente, se cuenta con un solo proyecto para discutir en la Asamblea Legislativa y que a mí criterio, tal y como lo exprese a lo largo de este trabajo, tiene grandes deficiencias. Algunas podrían ser corregidas para regular mejor y evitar futuros problemas.

e.- En Alemania, España, Estados Unidos y algunos países de habla hispana, en los cuales se ha implementado la firma digital, ha favorecido para que se dé el desarrollo de múltiples servicios, así como del comercio y transacciones en general.

f.- Para poder desarrollar e implementar el proyecto que hemos discutido a lo largo de la presente investigación, se debe tener el conocimiento básico y necesario en lo que respecta a términos, usos, tecnologías, etc.

g.- De aplicarse la figura de la firma digital, deberá capacitarse y entrenarse al personal para que este se desempeñe en sus labores de la mejor forma y logre el máximo aprovechamiento.

h.- Para la implementación de la firma digital debemos contar con los elementos y requisitos necesarios, detallados en la presente investigación.

i.- Con la implementación de la firma digital se obtienen múltiples beneficios al reducir las barreras de acceso a los mercados actuales.

j.- No obstante la sola promulgación de la ley, no significaría la implementación en los procesos y documentos judiciales, debido a que los mismos necesitarán de una mecánica judicial diferente que garantice su buen funcionamiento.

k.- De la discusión que se ha ido desarrollando entorno al proyecto, se deja ver que muchas de las empresas y compañías a las cuales se les ha solicitado su opinión, se mantienen al margen realizando un análisis al proyecto muy superficial y hasta subjetivo.

l.- El desarrollo de la firma digital, marcaría una pausa importante en la historia, debido a que se tendría que reformar y modificar algunos artículos que forman parte de nuestra normativa, sin mencionar la apertura mental que la gente deberá mantener.

En los últimos tiempos la informática ha dado un golpe a la realidad de nuestro país y el mundo entero, ha impulsado una sociedad sumamente dinámica, mientras por el contrario el derecho se ha caracterizado por ser una rama estática y conservadora. Esta visión del derecho debe cambiar, y ajustarlo a los adelantos tecnológicos, sin pretender estar a la vanguardia de estos, pero al menos cubriendo las necesidades y exigencias de la realidad del pueblo costarricense, con miras a crecer cada día más.

La intención de la presente investigación fue mostrar un poco la realidad del mundo en el cual convivimos día con día, así como la insuficiencia de nuestro ordenamiento y las soluciones dadas en otros países.

La oportunidad de implementar el Proyecto de "Ley de Firma Digital y Certificados Digitales" expediente 14.276, no puede quedar alejada de todas estas discusiones, pues sería un fracaso legislativo que a finales del siglo XXI nuestro ordenamiento no obstente ningún tipo de normativa al respecto, mientras que en muchos otros países tienen años de conocerla y desarrollarla.

La regulación oportuna debe ser la actitud por seguir en nuestro país de cara a evitar futuros tropiezos, garantizando de esta forma una mayor seguridad y eficacia jurídica.

Bibliografía

Libros Consultados.

- Comercio Electrónico en Internet, e-comerce, Universidad San Francisco Marroquín, Facultad de Ingeniería en Sistemas, Informática y ciencias de la Computación, Victoria del Rosario Pivaral Leal, Giovanni Obdulio Cajón Arrianza, Guatemala 2000.

- La Protección del Consumidor en el Comercio Electrónico, Jolene Marie Knorr y Marcelo Roldán Sauma, 1º edición, Editorial Investigaciones Jurídicas S.A., San José, Costa Rica julio del 2001.

- Proyecto de Guía para la incorporación al derecho interno de la ley modelo de la CNUDMI para las firmas electrónicas, Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 34 período de sesiones, Viena 25 de junio a 13 de julio de 2001.

- Ley Modelo de la CNUDMI sobre comercio electrónico con la Guía para su incorporación al derecho interno 1996, Naciones Unidas, Nueva York, 1997.

- Leyes y Negocios en Internet, Oliver Hance y Suzan Dionea Balz, Editorial McGraw-Hill Interamericana Editores, S.A. de C.V., México D.F.

- Legislación de Comercio electrónico, Ramón Casas Vallés y otros,Editorial Tecnos (Grupo Anaya, S.A.), 2001, Madrid España. Pág. 261-331.

- Proyecto de Ley, Ley de Firma Digital y Certificados Digitales, Expediente número 14.276, Asamblea Legislativa.

- Revista de Ciencias Jurídicas #97, Comercio Electrónico un breve acercamiento, Dr. Jorge Enrique Romero Pérez pág.123Facultad de Derecho enero-abril-2002.

- La Protección del Consumidor en el Comercio Electrónico, Jolene Marie Knorr y Marcelo Roldan, Pág. 52, 1 era Edición- San José Costa Rica IJSA julio de 2001.

- Diccionario Jurídico Elemental, Guillermo Cabanellas, Edición 1998, Editorial Heliasta.

- Procuraduría General de la República, Dictamen C-283-98, dirigido al Archivo Nacional el 24 de diciembre de 1998.

- Procuraduría General de la República, Dictamen C-015-95, 16 de enero de 1995.

- Procuraduría General de la República, Dictamen C-088-95, 17 de abril de 1998.

- Procuraduría General de la República, Dictamen C-139-99, 6 de julio de 1999.

- Informe Técnico, Proyecto de Ley, "Ley de Firma Digital y Certificados Digitales" Expediente Nº 14276, Oficio Nº 052-02-2002, Asamblea Legislativa de Costa Rica, Elaborado por la, Licda. Teresa Pérez Porta, diciembre de 2011.

- Voto 3495-92, Sala Constitucional de La Corte Suprema de Justicia, San José, a las catorce horas treinta minutos del diecinueve de noviembre de mil novecientos noventa y dos.

- La Nación, Gran potencial en Internet Abrirán certificadora de firmas digitales Édgar Delgado M, Lunes 3 de diciembre, 2001. San José, Costa Rica.

- Comentarios acerca de las deficiencias que presenta él Proyecto de Ley sobre la Firma Digital, Revista Número 1, 20 de junio del 2001, Licenciado Guillermo Augusto Pérez Merayo, Profesor de Derecho Informático Facultad de Derecho, Universidad de Costa Rica.

- Comentario al Libro "Firma Digital y Derecho Societario Electrónico", Bernardo P. Carlino(Un volumen de 232 ps., Ed. Rubinzal-Culzoni, Sta. Fe, 1998, con prólogo de Héctor Alegría).

- Derecho Mercantil Contemporáneo, Comercio Electrónico, Firma Digital y Autoridades de certificación, Segunda Edición, Apol.nia Martínez Nadal, Civitas Ediciones: SL 2000, paginas 27 al 87, 123 al 217.

- Comercio Electrónico, Arbitraje Comercial Internacional Garantías Independientes. Concurrencia la hora del balance, Ana Isabel Piaggi, Luis Alejandro Estoup, La Ley S.A. Tucuman 1471 Buenos Aires Argentina 2001.

- El Documento Informático en su óptica notarial, civil y penal y su seguridad jurídica, Tesis de Licenciatura en derecho, Universidad de Costa Rica, Raul Antonio Segnini Zamora, 1995.

- Constitución Política de la República de Costa Rica, Lic. Marco Castillo Rojas, Editores Uruk, Cartago Costa Rica 1996.

- Código de Comercio de la República de Costa Rica, Editorial Porvenir 1999.

- Código Notarial de la República de Costa Rica, Herman Mora Vargas, Investigaciones Jurídicas S.A., julio 2000.

- Código Civil de la República de Costa Rica, Gerardo Parajeles Vindas, Investigaciones Jurídicas S.A., febrero 2001.

- Código Procesal Civil de la República de Costa Rica, Gerardo Parajeles Vindas, Investigaciones Jurídicas S.A., setiembre 1999.
- Código Penal de la República de Costa Rica, Ulises Zúñiga Morales, Investigaciones Jurídicas S.A., febrero 2001.

Seminarios asistidos.

- Seminario Impartido en La Universidad Latina de Costa Rica, el día 18 y 19 de junio del 2003, por el MS.c Edwin Aguilar Sánchez.

- Seminarios de Firma Digital en la Función Notarial y Registral, Universidad de Costa Rica, Facultad de Derecho, expositores: Dr. Agustín Viguri Perea, Catedrático de la Universidad Jaume I, España y el Master Frank Rosich, Consultor certificado por la IBM en Negocios Electrónicos.

Direcciones electrónicas.

- Lic. Daniel Edgardo Cortés, www.certificadodigital.com.ar, http://www.fundaciondike.org/seguridad/firmadigital.html

- La Firma Digital y sus consecuencias dentro de los marcos jurídicos actuales, José de Jesús Angel Angel, director de Investigación y Desarrollo de SeguriDATA,Http://www.htmlweb.net/seguridad/varios/ firma_juridico.html

- Firma electrónica, AGM – LAWROPE- Abogados, Departamento de Derecho Civil – Mercantil, http://www.efranquizium.com/articulos/ nuevas_ tecnologias/agm.asp

- Temas de Derecho: El documento electrónico, sistemas de autenticación y la firma digital, Dirección Dr. Mauricio Devoto, http://www.it-cenit.org.ar/Seminarios/DerEconDIG2000/material/ EDoc/Leyes.htm

- España pionera en Europa al aprobar el uso de la firma notarial electrónica, 20 de mayo de 2002,http://www.virusprot.com/ Nt200532.html

- Servicios y Aplicaciones de la Firma Electrónica, Rodolfo Lomascolo, r.lomascolo@mail.ips.es, www.ipsCA.com

- Firma y Certificado Digital Universidad del Salvador (ARGENTINA) - Georgetown University (USA) Catedra Marco legal Año 2001, http://www.hfernandezdelpech.com.ar/Leyes/TRABAJO%20FIRMA% 20DIGITAL%20POSTGRADO%20E.-BUSINESS.htm

- Funcionamiento de la Firma electrónica, http://www.informatica-juridica.com/trabajos/aspectos_tecnicos.asp

- Gobierno digital: un paso hacia la digitalización de Costa Rica Por: Hernando Pantigoso Asesor área de Tecnología del Consejo de Asesores Presidenciales y encargado de la Agenda Digital Miembro de las Juntas Directivas del ICE y RACSA, http://www.go.cr/esp/gobiernodigital.html

- Guía Temática, http://www.diputados.gov.ar/guia_tematica.html

- Guía Sobre el Uso y Eficacia deLa Firma Electrónica, http://www.mju.es/guia_f_elect.htm

- Internet Banking será el Canal de Distribución por Excelencia, Año XIII/ Número 9/ Abril-Mayo, 2000 Rodolfo Gasparri, http://www.bancomercantil.com/actual/noticias/noticias_mercantil/200005/pag3.html

- El Mundo Real por Cristina Hernández Trejo Seguridad digital, otro plus de la Factura Electrónica, http://www.amece.org.mx/boletines/oct-nov/headers.php?pag= mundo

- La Firma Digital y Entidades de Certificación (José Cuervo), http://www.informatica-juridica.com/trabajos/firma_digital.asp

- La firma electrónica en el Derecho privado, Dr. Luis Fajardo López, Prof. Asoc. de Derecho civil de la Universidad de Gerona, http://www.fajardolopez.com/materiales/Fajardo_RJUAM.html

- La firma electrónica y los Registros, http://www.notariadigital.com/ boletin013.htm

- La Firma y El Comercio Electrónico. http://www.mju.es/g_ firmaelect_ amp.htm#

- "La influencia de la informática en la actividad probatoria y su regulación en Uruguay "Dra. Esc. María José Viega Rodríguez, http://www.derecho.org/comunidad/mjviega/actprob.htm

- Firma real en un mundo virtual, http://www.estudioluzclara.com/ Interior/DerechoInformatico

- PREGUNTAS Y RESPUESTAS, http://www.senacyt.gob.pa/firmadigital/ preguntasrespuestasiv.htm

- Problemas, ventajas, mentiras y promesas de la historia electrónica, http://www.diariomedico.es/gestion/ges210501com.html, Laura G. Ibañes

- Legislacion Basica Sobre Telecomunicaciones, Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica,http://www.setsi.mcyt.es/legisla/internet/rdley14_99.htm

- Estados Unidos apuesta por el comercio electrónico, 4 de julio de 2000,http://www.expansiondirecto.com/2000/07/04/tecnologia/4tec.html

- Estudio de situación del comercio electrónico en España, http://www.internautas.org/documentos/pista.htm

- Entrevista a Eduardo Krell W, ocho de mayo del dos mil dos, Patricia Andrade, http://www.clcert.cl/pipermail/info/2002-May/000012.html

- La Asociación Gestiona su Firma Electrónica http://www.lasasesorias.com/es/publica/firmaelectronica/

- Firmas Digitales, http://www.diputados.gov.ar/guia_tematica2.html Comercio electrónico, http://mailweb.udlap.mx/~is104418/Antecedentes.html

- El Comercio Electrónico Global, http://www.arrakis.es/~anguiano/ artcomglobal.html

- Instituto Nacional de Estadística e Informática ¿QUÉ ES EL COMERCIO
- ELECTRÓNICO?http://www.uap.edu.pe/fac/02/enlaces/manual htmlegl/inei/Libro-5104.pdf

- Firma Electrónica Y Documentos Digitales Angelo Benvenuto V. abenven@udec.cl

- Análisis Comparativo de La Legislación y Proyectos a Nivel Mundial Sobre Firmas y Certificados Digitales (distintas soluciones), Por Hugo Daniel Carrion, http://www.informatica-juridica.com/trabajos/ analisis_comparativo_a_nivel_mundial_sobre_firma_digital.asp

- La seguridad elemento fundamental en la era de internet, Emilio Palomar del AMO Director General SIA, Sistemas Informáticos Abiertos, jmcugat@sia.es

- Comentarios al Proyecto de Ley de Firma Digital de Costa Rica, Por Christian Hess A. http://comunidad.derecho.org/chess/ publicac/firmadigital.html

- Gobierno digital: un paso hacia la digitalización de Costa Rica Por: Hernando Pantigoso, Asesor área de Tecnología del Consejo de Asesores Presidenciales y encargado de la Agenda Digital

Miembro de las Juntas Directivas del ICE y RACSA, http://www.micit.go.cr/adn/pdn.php

- Debatieron el futuro y la seguridad de la firma digital, pagina 21, http://www.rt-a.com/68/21-68.htm

- Comercio Electrónico en América Latina, Realidades y Perspectivas
- Por Erick Iriarte Ahon, Alfa-Redi. Revista de Derecho Informático (Artículos sobre E-commerce). http://www.alfa-redi.org

- Conclusiones Generales de La Comision de Firma Digital, http://www.aadat.org/conclusiones_generales42.htm

- El desarrollo verdadero del Internet en Costa Rica, 16 de abril de 2001, http://www.tiquisia.com/editorial/index15.asp

- Destacan aprobación de proyecto de ley de firma electrónica, http://www.lasemanajuridica.cl/LaSemanaJuridica/793/article-5845.html

- Firma Electrónica, Universidad Tecnológica Metropolitana, septiembre de 2002, http://www.utem.cl/cyt/derecho/firma.html

- FIRMA DIGITAL, http://www.delitosinformaticos.com/ecommerce/contratos.shtml12 de Enero 2002

- Una Estrategia Nacional en el Desarrollo de Las TICs y El Comercio Electrónico: La Experiencia de Costa Rica, Ministerio de Comercio Exterior (COMEX)mpicado@comex.go.cr junio 2002

- Firma electrónica, Adiós al papel, Domingo 7 de abril de 2002 Paola PassigV,http://www.mercuriovalpo.cl/site/apg/reportajes/pags/20020406235922.html

- Informática, Blanch, Leonardo, Cabrera, Federico M,Cafure, Martín J. www.monografias.com

- Ley del Estado de UTA, sobre la Firma digital, www.cnv.gov.ar/FirmasDig/Internacional/lutah.html
- Respuestas a las preguntas mas frecuentes sobre Criptografía actual, www.cnv.gov.ar./FirmasDig/RSAFaq.html.

- Legislación Básica sobre Telecomunicaciones, Real decreto Ley 14/1999, de 17 de setiembre, sobre firma electrónica, www.setsi.mcyt.es/legisla/internet/rdley14_99.html

- Firma Electrónica, Cámaras de Comercio presentan su sistema de certificación digital: la camerfirma, www.camerfirma.com

- Banca, comercio, moneda electrónica y la firma digital, www.notariadigital.com/boletin004.htm

- Y donde esta el delito, www.monografias.com

- Banca, comercio, moneda electrónica y la firma digital, Mauricio Devoto y Horacio M. Lynch, www.it-cenit.org.ar/Publicac/BancaMD/banCom6

- Como aplicar la nueva normativa sobre la Firma electrónica, Fernando Ramos Suárez, Febrero 2002, www.legalia.com

- Documento Electrónico, www.monografias.com

- Palazi(Pablo) y Peña (Julián), Comercio Electrónico y MERCOSUR, Documento sin numeración disponible en http://publicaciones.derecho.org/redi/intex.c.gi?N%

- Federal Trade Commission, Internet Pyramid Surf a Day Report, Diciembre 1996. Disponible en http//www.ftc.gov.

RESUMEN EJECUTIVO.
LA FIRMA DIGITAL DENTRO DE LAS TRANSACCIONES COMERCIALES.

La ley es indispensable para el desarrollo social, cumpliendo la misión de regular los derechos y obligaciones de los ciudadanos de uno o varios países, es por esto que debe cambiar constantemente y adecuarse a la realidad latente de ese momento, sobre todo cuando la tecnología ha avanzado tanto que prácticamente le exige un cambio.

"La doctrina jurídica conviene en que la firma es el género, la firma electrónica una especie y dentro de ésta encontramos subespecies, tales como las denominadas en algunas legislaciones como firma digital, firma electrónica avanzada, ó firma electrónica certificada".[195]

En esta investigación el objetivo principal fue el estudio de esta figura que hemos denominado **"Firma Digital",** en su óptica notarial, civil y comercial, con el fin de demostrar que esta constituye un verdadero elemento tecnológico, legal, valido y eficaz, para la realización de transacciones electrónicas que garanticen seguridad, confidencialidad y agilidad dentro del comercio electrónico, siguiendo con los patrones legales propuestos.

De conformidad con el trabajo de investigación se entenderá como firma digital el "Bloque de caracteres que acompaña a un documento (o fichero) acreditando quien es su autor **(autenticación)** y que no ha existido ninguna manipulación posterior de los datos **(integridad)**. Para Firmar un documento digital, su autor utiliza su propia clave secreta **(sistema Criptográfico asimétrica)**, a la que solo tiene acceso, lo que impide que pueda después negar su autoría **(no-revocación o no repudio)**. De esta forma, el autor queda vinculado al documento de la firma. Por ultimo la validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor."[196]

Dentro de los objetivos generales en está investigación tenemos: **I.-**Analizar el proyecto de Ley de Firma Digital y Certificados Digitales expediente 14.276 según parámetros de legislación y doctrina comparada y **II.-**Diseñar propuestas al texto

[195] Conclusiones generales de la comisión de firma digital, Dra. Gabriela Guerriero, Dr. Mario Maio, Dra. Marina Mongiardino, Dr. Diego Rull, Dra. Carolina Vega, Dra. Mercedes Velásquez, http://www.aadat.org/conclusiones_generales42.htm

[196] Como Aplicar la nueva normativa sobre la firma electrónica, Fernando Ramos Suárez, Febrero 2000, Documento disponible en Internet: http://www.legalia.com

sustitúyete del Proyecto 14.276, que permita una posible aplicación de la Firma Digital. En cuanto a los objetivos específicos, se plantearon de conformidad con los anteriores los siguientes: **a)**determinar la correcta utilización del lenguaje técnico; **b)**identificar con otras experiencias comparadas la regulación de deberes y derechos de las entidades certificadoras; **c)**hacer un listado de requisitos mínimos que se debe de tener para lograr utilizar la firma digital; **d)**identificar a las autoridades competentes para la regulación de la Firma Digital; **e)**descubrir los vacíos de regulación que existen dentro del proyecto de ley expediente catorce mil doscientos setenta y seis; **f)**valorar la legislación y doctrina posiblemente aplicable en Costa Rica; **g)**desarrollar a fondo la firma digital para evitar los vacíos de regulación; **h)**justificar las propuestas que posiblemente vayan a modificar el proyecto de ley expediente catorce mil doscientos setenta y seis; **i)**diseñar un posible texto sustituyente.

Asimismo se referirá a las transacciones comerciales que se podrían realizar en Costa Rica, de estar aprobada una ley sobre firma digital tales como: **1.**Reducción de las barreras de acceso a los mercados actuales; **2.**Reduce o incluso elimina por completo los intermediarios; **3.**Brinda información rápida y precisa en el lugar indicado; **4.**Permite un mejor planeamiento de la recepción y el despacho de mensajes; **5.**Seguridad en el procesamiento de transacciones, se eliminan los errores por el reingreso de información; **6.**Reducción de costos administrativos; **7.**Disminuye notablemente la cantidad de documentos impresos; **8.**Comunicación permanente las 24 horas los 365 días del año, entre otras.

Con respecto al proyecto de ley 14276 que existe actualmente en nuestra Asamblea Legislativa denominado "**Ley de Firma Digital y Certificados Digitales"** cuyo objetivo es "*dar validez jurídica a la firma digital y autorizar al Estado para su utilización. (artículo 1)"*[197], se realizo junto a doctrina aplicable y experiencia comparada un análisis del mismo, con el cual se podrá identificar de manera un poco más clara algunas deficiencias que presenta este proyecto.

El trabajo de investigación esta dividido en tres títulos. Cada título consta de dos capítulos a excepción del último título que solamente posee un capítulo, que a su vez contienen varias sesiones.

El primer título se denomina **Generalidades de la Firma Digital y su Relación con el Derecho**, dentro del cual se desarrollaran temas como antecedentes, nociones generales, origen y evolución de la firma, así como su desarrollo en nuestro territorio. Este primero es de suma importancia debido a que es en este título, donde se crean las bases para la efectiva comprensión del tema.

El segundo título es denominado **Técnicas y Usos de la Firma Digital dentro de las Transacciones Comerciales**, dentro del cual se desarrollan puntos importantes como técnicas y usos de la firma digital, elementos, requisitos y

[197] María Teresa Bermúdez, Adolfo Barquero, Danilo Retana y Ana Lucía Jiménez, Informe a la Dirección General del Archivo Nacional respecto a la posición tomada hacia el proyecto de ley 14276, Asamblea Legislativa Expediente 14276, folio 47.

métodos, ventajas y desventajas, así como sus aplicaciones sobre distintos documentos.

El tercer título es denominado **Análisis del proyecto de Ley 14276 "Ley de Firma Digital y Certificados Digitales"**, junto a doctrina y experiencia comparada, desarrollándose en este último título las consideraciones al proyecto, doctrina aplicable, análisis del articulado y nueva propuesta la cual surgió con el desarrollo de la investigación debido a que se encontraron deficiencias en el proyecto mencionado las cuales consideró deben de modificarse con el fin de evitar futuros tropiezos.

La oportunidad de implementar el Proyecto 14.276, no puede quedar alejada de todas estas discusiones, pues sería un fracaso legislativo que nuestro ordenamiento no ostenté ningún tipo de normativa al respecto, mientras que en muchos otros países tienen años de conocerla y desarrollarla.

ANEXO 1

PROYECTO DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES.

PRIMERA VERSIÓN.

PROYECTO DE LEY

LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

Expediente Nº 14.276
Primera Versión

ASAMBLEA LEGISLATIVA:

La comunicación entre los seres humanos, particularmente las comunicaciones a distancia se han facilitado conforme avanza la tecnología. El telégrafo, el teléfono, la radio, la televisión, el fax, cada uno a su tiempo, han representado importantes pasos en materia de comunicación humana, y han conformado una base tecnológica de mucha capacidad, la cual ha iniciado una verdadera revolución en las comunicaciones y el desarrollo de las sociedades contemporáneas. Una de las áreas más beneficiadas con estas nuevas y ágiles herramientas de comunicación es la del comercio. Por su misma naturaleza, requiere cada vez más de mecanismos ágiles y eficientes pero también seguros de comunicación.

Esta cadena de logros tecnológicos en materia de comunicación ha alcanzado un punto muy alto con la extensión de la red internacional o Internet (red de redes), la cual ha ampliado exponencialmente las posibilidades y facilidades de comunicación entre los seres humanos. Es, definitivamente, un medio que no puede ser ignorado por ninguna persona, mucho menos por el sector comercial alrededor de todo el orbe. Y en efecto, no lo ha sido. Los expertos coinciden en afirmar que la Sociedad de la Información ha encontrado en Internet el canal de flujo ideal, por sus preciados atributos: rápido, barato, y cada vez más extendido y eficiente. Cada vez más empresas deciden incursionar en el mercado virtual, y basan sus comunicaciones externas en ella; igualmente, con más pausa y mesura pero con la misma decisión, los operadores financieros comienzan a utilizar el nuevo medio. Y no podría ser de otra forma ya que en el mercado virtual adquieren ventajas comparativas que sencillamente no existen en el mundo físico, siendo la reducción de costos uno de sus principales beneficios. Es notable que este tipo de instrumento accesible actualmente a una parte de la población, era accesible hasta hace pocos años, únicamente a las corporaciones más poderosas del planeta. La pequeña y mediana empresa ven en efecto en la Internet la posibilidad de un acceso sin precedentes a la información y los mercados mundiales a un costo reducido, y con tendencia a bajar, no a subir, a medida que la red de redes se extiende en todo el orbe. Estamos presenciando una verdadera revolución en el acceso al conocimiento, a la información y la comunicación con consecuencias apenas imaginables para el futuro de la humanidad.

Para las economías en desarrollo como la nuestra, el maximizar los beneficios que ofrece el comercio electrónico es un imperativo; pero también es lograr una posición de vanguardia en la transferencia de tecnología e información, con base al potencial que tiene nuestro país en cuanto a recursos humanos calificados en el área informática, tecnológica y profesional, en general.

El resultado de este proceso ha sido el advenimiento de la Economía Digital, en la cual el valor recae con mayor fuerza en bienes intangibles, y en el conocimiento. Pero también ha significado una nueva vía amplísima y dinamizadora de comercio.

El desarrollo del comercio electrónico ha sido vertiginoso, sin embargo, presentará obstáculos difíciles de superar si no se resuelven ciertos aspectos técnicos y de índole legal. Desde el punto de vista jurídico esta revolución tecnológica e informática ha significado un reto complejo y desafiante: dotar de seguridad jurídica el tráfico, tanto de información como de bienes y servicios. La contratación electrónica debe ser objeto de regulación, en forma muy cuidadosa, para que las nuevas tecnologías de la información no se vuelvan inoperantes. Uno de los temas esenciales a tratar, si no el más importante, es el del reconocimiento legal de la Firma Digital. No es posible concebir un creciente desarrollo del comercio electrónico, y la incursión de otro tipo de transacciones jurídicas en la red, si no se provee de la adecuada seguridad para el normal desempeño de estas actividades. La Firma Digital es un mecanismo concebido en función de esta meta prevaleciente, y es objetivo del presente proyecto regularla de forma tal, que existan los elementos jurídicos fundamentales para el desarrollo de la Economía Digital en un contexto razonable, mas no infalible, de seguridad jurídica, estimulando el poder de su "motor": el comercio electrónico.

Este proyecto de ley es coherente con el derecho internacional en tema de comercio electrónico, con el propósito de obtener la adecuada seguridad y certidumbre en las transacciones electrónicas basadas en la red de redes. La importancia que reviste la uniformidad respecto al tratamiento de los aspectos más importantes sobre comercio electrónico, es insoslayable. La regulación propuesta pretende mantener la armonía con los elementos principales de la regulación internacional sobre el tema, brindando el marco jurídico adecuado y viable para la contratación electrónica, y en general, las relaciones jurídicas basadas en la comunicación mediante medios informáticos o telemáticos, sean o no de índole comercial. Esto se haría entonces, esencialmente, a través del reconocimiento de eficacia, desde el punto de vista probatorio, de la Firma Digital vinculada a un proveedor de servicios de certificación.

Debe despejarse cualquier duda respecto de la validez jurídica como prueba del documento electrónico, el cual, de conformidad con nuestra legislación procesal civil, es admisible como prueba en sede jurisdiccional.

En concreto, para lograr los objetivos supracitados es preciso: regular el reconocimiento legal expreso de la Firma Digital; determinar los efectos de la Firma Digital; el reconocimiento del principio de equivalencia funcional por medio del cual se confiere al documento digital firmado los mismos efectos que se le imputan al documento escrito; acoger el "principio de neutralidad tecnológica", de forma tal que la normativa no limite el mecanismo de Firma Digital a una sola tecnología; establecer reglas mínimas en materia de conservación, envío y recepción de mensajes de datos para aquellos casos en que las partes no hayan estipulado reglas especiales.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

TÍTULO I
PRINCIPIOS Y NORMAS GENERALES
CAPÍTULO PRIMERO
DISPOSICIONES GENERALES

ARTÍCULO 1.- La presente Ley tiene por objetivo regular el uso y el reconocimiento jurídico de la Firma Digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como el autorizar al Estado para su utilización.

ARTÍCULO 2.- Para los propósitos de la presente Ley se establecen las siguientes definiciones:

Acreditación: La acreditación es el procedimiento mediante el cual un organismo autorizado reconoce formalmente que una entidad o empresa es competente para realizar tareas específicas.
Acreditación voluntaria del prestador de servicios de certificación: Resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se emite, a petición del interesado, por el Órgano Rector y la Autoridad Competente de acreditación, de conformidad con lo previsto en esta Ley, su reglamento y la normativa intencional aplicable.
Certificado Digital: Es la certificación digital que vincula unos datos de verificación de firma a un signatario y confirma su identidad.
Certificado Digital Reconocido: Es el certificado que cumple con los requisitos establecidos en la presente Ley y su reglamento, y que vincula un documento digital con determinada persona como su signatario, mediante un proceso seguro de certificación y es expedido por un prestador de servicios de certificación acreditado por el Órgano Rector y la autoridad competente de acreditación.
Datos de creación de firma: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la Firma Digital.
Datos de verificación de firma: Son los datos como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma Digital.
Dispositivo de creación de firma: Es un mecanismo que sirve para aplicar los datos de creación de firma.
Dispositivo de verificación de firma: Es un mecanismo que sirve para aplicar los datos de verificación de firma.

Dispositivo seguro de creación de firma: Es el mecanismo de creación de firma que cumple adicionalmente con los requisitos establecidos en la presente Ley y su reglamento.
Documento: Significa información que se encuentra almacenada en un medio tangible, o que se guarda en un medio electrónico o de cualquier otra naturaleza, y que se puede recuperar o reproducir en una forma perceptible e inteligible.
Firma Digital: Es el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.
Firma Digital Avanzada: Es la Firma Digital Certificada por un prestador de servicios de certificación debidamente acreditado ante la autoridad competente de acreditación.
Información: Es aquel mensaje comunicado mediante datos, textos, imágenes, sonidos, códigos, programas, información almacenada en bases de datos, aplicaciones, o similares.
Iniciador: Es quien envía un mensaje de datos, esté o no suscrito digitalmente.
Información Íntegra: Se entenderá por íntegra aquella información que haya permanecido completa e inalterada, sin menoscabo de cualquier adición o cambio, inherente al proceso de comunicación, almacenamiento, archivo o presentación. El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.
Intermediario: Es aquella persona, física o jurídica, que actuando por cuenta de otra, envíe, reciba, almacene dicho mensaje o preste algún otro servicio con respecto a él.
Mensaje de datos: Es la información generada, enviada, recibida, almacenada, o comunicada por medios digitales, electrónicos, ópticos o similares.
Prestador de servicios de certificación o entidad certificadora: Es la persona física o jurídica que expide certificados.
Procedimiento seguro: Es el procedimiento empleado con el propósito de verificar que una Firma Digital es atribuible a determinada persona como su signatario, o para detectar cambios y errores en un documento digital, incluyendo cualquier proceso que implique el uso de algoritmos matemáticos, códigos, sistemas de encriptamiento, y cualquier otro medio o tecnología de identificación o reconocimiento.
Producto de Firma Digital: Es el instrumento y sus componentes específicos, destinados a la prestación de servicios de Firma Digital por el prestador de servicios de certificación o para la creación o verificación de Firma Digital.
Receptor: Es la persona a quien el signatario dirige el mensaje o documento electrónico.
Signatario: Es la persona física o jurídica que cuenta con un mecanismo de creación de firma, que actúa en nombre propio o con poderes de representación de otra persona física o jurídica.
Sistema: Es el conjunto de elementos independientes pero interrelacionados entre sí para conseguir un propósito común.

Sistema de información: Es un conjunto de elementos ordenado utilizado para generar, enviar, recibir, almacenar o procesar de alguna forma mensajes de datos.

ARTÍCULO 3.- En la presente Ley se utilizará el término digital entendido como cualquier información codificada en dígitos, la cual resulta más precisa que el término electrónico, que se refiere al medio físico de procesamiento, almacenamiento o transmisión, el cual es uno de los medios para generar, transmitir y almacenar información digital.

CAPÍTULO II
RECONOCIMIENTO JURÍDICO DE LA FIRMA DIGITAL

ARTÍCULO 4.- La Firma Digital Avanzada, deberá crearse mediante un dispositivo seguro de creación de firma.

ARTÍCULO 5.- La Firma Digital Avanzada, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel.
Cuando la ley exija la presentación o existencia de un documento escrito debidamente firmado, tal requisito será plenamente satisfecho por un documento digital, si el mismo ha sido firmado mediante una Firma Digital Avanzada, creada por un dispositivo seguro de creación de firma.
Se presumirá que la Firma Digital Avanzada y el medio de creación de firma con el que ésta se produzca, reúnen las condiciones necesarias para producir los efectos indicados en este apartado cuando el certificado reconocido es emitido por un prestador de servicios de certificación acreditado.

ARTÍCULO 6.- Cuando una ley requiere que un documento o firma esté certificado o autenticado notarialmente por un abogado, o de cualquier otra forma reconocido, verificado o certificado, tal requisito se tendrá por cumplido si una firma electrónica avanzada de un notario público, abogado, funcionario público, o cualquier otra persona autorizada y competente para efectuar tales actos, es puesta o vinculada al documento o firma digital o Firma Digital avanzada.

CAPÍTULO III
USO DE LA FIRMA DIGITAL Y LOS DOCUMENTOS
ELECTRÓNICOS POR EL ESTADO

ARTÍCULO 7.- Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, Contraloría General de la República, Defensoría de

los Habitantes, así como a todas las instituciones públicas descentralizadas, y entes públicos no estatales para la utilización de la Firma Digital avanzada y los documentos electrónicos firmados digitalmente en sus relaciones internas, entre ellos y con los particulares, de conformidad con las previsiones de esta Ley y su reglamento.

TÍTULO II
DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL
CAPÍTULO I
DEL ÓRGANO RECTOR

ARTÍCULO 8.- El Ministerio de Ciencia y Tecnología será el Órgano Rector en todo lo concerniente a esta Ley.

8.1 Toda interpretación técnica estará bajo el mejor criterio del Órgano Rector tomando en cuenta el estado de arte en la tecnología, así como los requerimientos y realidades del país.

ARTÍCULO 9.- El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizará un sistema de acreditación voluntario, en el ámbito de los prestadores de servicios de certificación de Firma Digital Avanzada, coordinando para ello con la Autoridad de Acreditación, la cual será un ente con participación activa y equilibrada de los sectores involucrados. La autoridad de acreditación mediante la función de acreditación, reconoce formalmente que una organización es competente para llevar a cabo tareas específicas de acuerdo a los requisitos de normas nacionales e internacionales, que permitan lograr un adecuado grado de seguridad y confianza que proteja debidamente, los derechos de los usuarios, para lo cual deberá llevar a cabo el proceso de evaluación correspondiente, un registro de las entidades acreditadas y velar por que se cumplan los requisitos establecidos por esta Ley y su reglamento.

CAPÍTULO II
CERTIFICADOS DIGITALES

ARTÍCULO 10.- Los certificados digitales se vinculan con una persona confirmando su identidad, los cuales deberán contener al menos:

Los datos que identifiquen individualmente al firmante.
Los datos que identifiquen a la entidad de certificación.
Número de serie del certificado.
Fecha de emisión y plazo de vigencia.
Los demás que el reglamento establezca.

ARTÍCULO 11.- Los certificados digitales se podrán cancelar y revocar en los siguientes casos:

A solicitud del titular de la firma.
Por expiración del plazo.
Por cese de operaciones de la entidad de certificación.
Por muerte del titular de la Firma Digital.
Por incumplimiento contractual con la entidad de certificación.
Las demás que el reglamento establezca.

ARTÍCULO 12.- Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por prestadores establecidos en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y reconocidos por la autoridad de acreditación competente y cumpliendo con los requisitos fijados en esta Ley, su reglamento y normas internacionales correspondientes.

CAPÍTULO III
DE LA ACREDITACIÓN E INSPECCIÓN DE LOS PRESTADORES
DE SERVICIOS DE CERTIFICACIÓN DIGITAL

ARTÍCULO 13.- Mediante la autoridad competente de acreditación, la cual estará adscrita al Ministerio Rector, las empresas que emitan certificados de Firma Digital, deberán someterse al proceso de acreditación que se defina al respecto para estar debidamente acreditados. Las funciones de las empresas certificadoras serán entre otras las de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado.

ARTÍCULO 14.- Con el fin de comprobar el cumplimiento de las obligaciones de los prestadores acreditados, la Autoridad de Acreditación ejercerá la facultad de inspección sobre los prestadores acreditados y podrá, a tal efecto, requerir información, ordenar evaluaciones anunciadas o no anunciadas a sus instalaciones al menos una vez al año y solicitar las modificaciones necesarias para que se mantenga actualizado el sistema y el servicio, con personal que para tal efecto se seleccione de conformidad al reglamento, la Autoridad de Acreditación y del Órgano Rector. Así como suspender las acreditaciones en caso de incumplimiento.

ARTÍCULO 15.- La Autoridad de Acreditación así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen las empresas certificadoras.

ARTÍCULO 16.- El Órgano Rector deberá observar en sus actuaciones y regulaciones total neutralidad respecto de las diversas tecnologías de Firma Digital existentes, procurando la mayor adaptabilidad a los avances científicos y tecnológicos en tal área.

TÍTULO III
LOS DISPOSITIVOS DE FIRMA DIGITAL AVANZADA Y LA EVALUACIÓN DE SU CONFORMIDAD CON LA NORMATIVA APLICABLE

CAPÍTULO ÚNICO

ARTÍCULO 17.- Los dispositivos seguros de creación de Firma Digital para considerarse como tales deberán cumplir con:

Garantizar que los datos utilizados para la generación de firma puedan producirse sólo una vez y asegurar, razonablemente, su secreto, dentro de las posibilidades o limitaciones tecnológicas.
Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados con la tecnología existente en un momento dado.
Que los datos de creación de firma puedan ser protegidos con fiabilidad por el signatario contra la utilización por otros.
Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que éste se muestre al signatario antes del proceso de firma.

ARTÍCULO 18.- Los dispositivos de verificación de Firma Digital Avanzada deben garantizar al menos lo siguiente:

Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.
Que el verificador pueda, en caso necesario, establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.
Que aparezca correctamente la identidad del signatario.
Que se verifique de forma fiable el certificado.
Que pueda detectarse cualquier cambio relativo a su seguridad e integridad.

ARTÍCULO 19.- Las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte.

TÍTULO IV
DISPOSICIONES FINALES

ARTÍCULO 20.- El Poder Ejecutivo deberá emitir el reglamento a la presente Ley dentro del plazo máximo de tres meses siguientes a su publicación.

Rige a partir de su publicación.

Miguel Ángel Rodríguez Echeverría
PRESIDENTE DE LA REPÚBLICA

Guy de Téramond
MINISTRO DE CIENCIA
Y TECNOLOGÍA

22 de febrero de 2001, gdph.

NOTA: Este proyecto pasó a estudio e informe de la Comisión Especial de Propiedad Intelectual.

ANEXO 2

DICTAMEN DE LA PROCURADURÍA

C-283-98

PROCURADURIA GENERAL DE LA REPUBLICA
Sistema Nacional de Legislación Vigente (SINALEVI)

San José, Costa Rica

DICTAMEN C-283-98
24 de diciembre de 1998.

Señora
Licda. Ana Virginia García de Benedictis
Subdirectora
ARCHIVO NACIONAL

Estimada señora:

Con la debida aprobación del señor Procurador General de la República, me es grato dar respuesta a su atento oficio SD-6989 donde nos consulta sobre la validez probatoria del documento electrónico escrito en disco compacto.

Como apoyo de su consulta acompaña la opinión de la Licenciada Argerie Díaz Rojas, Asesora Legal de esa Institución, en que plantea

algunas reservas al respecto, tal como nos lo señala Ud. en la consulta cuyo tenor transcribimos textualmente:

"Las dudas básicamente están relacionadas al uso de la tecnología de discos ópticos, para el almacenamiento de documentos del Archivo Nacional, el sustento legal está apoyado en el artículo 3º de la Ley 7202, en el artículo 368 del Código Procesal Civil y otros de los cuales se puede desprender que nuestro derecho positivo no le da valor legal a los documentos electrónicos, ya que no pueden reunir en su totalidad, los requisitos de documento público: sobre todo poniendo énfasis en el aspecto procesal, especialmente el probatorio.

Se pone énfasis, en cuanto que sería contraproducente sustituir al documento escrito en el papel por otras formas, tal es el caso del disco óptico, por cuanto no hay una posición clara en su valor como prueba legal.

Por tanto, mucho le agradecería, emitir la opinión jurídica de esa Procuraduría en cuanto a la validez del documento

"escrito" en disco óptico o cualquier otro lenguaje electrónico; ya que nuestra mayor inquietud como lo hemos dicho anteriormente, es su valor de prueba".

INTRODUCCION

Hasta hace muy pocos años, el papel y la escritura eran los soportes naturales en los que se formalizaban todos los documentos. El desarrollo y la amplia difusión de la Informática han modificado tal circunstancia irrumpiendo fuertemente en los usos y costumbres de las actividades gubernamentales, las prácticas comerciales y en la vida diaria de los ciudadanos.

En efecto, el acelerado proceso de informatización va generando paulatinamente el reemplazo del documento escrito por el documento electrónico. Tanto en la Administración Pública como en la actividad privada la aplicación informática se va generalizando en todos sus respectivos sectores.

Todos los aspectos de nuestra vida actual se han ido transformando con la utilización de la computadora, produciendo cambios sociales, que ponen en evidencia que la cultura escrita va cediendo paso a un nuevo mundo, en el que predominará la transmisión electrónica de datos y donde ocuparán un lugar preponderante las comunicaciones (denominadas las autopistas del nuevo milenio).

Por ello es de extraordinaria importancia para la vida institucional no sólo del Archivo Nacional sino del país en general, la regulación que

adopte respecto del disco compacto, ya que como garante del patrimonio documental costarricense le corresponde tomar todas las previsiones para incorporar eficientemente todo el acervo documental que las nuevas tecnologías de la información proveen.

Con el fin de evacuar la cuestión planteada, hemos considerado conveniente explicar algunos conceptos de Informática, con el objeto de puedan precisar posteriormente nuestras preocupaciones sobre las regulaciones que se deben implementar para dotar a los documentos electrónicos de las características deseadas de seguridad y de valor jurídico que como documento deben llenar.

El almacenamiento computadorizado de la información

El primer aspecto que hay que explicar es sobre la escritura de un documento informático o sea como se escribe y se guarda un documento producido en o por medio de una computadora, y como se almacena y reproduce posteriormente.

Toda computadora está compuesta de dos partes: su cerebro que es el microprocesador, y los dispositivos auxiliares. El almacenamiento de la información es de dos tipos: interno o primario (dentro del microprocesador) y externo (en los dispositivos auxiliares).

El almacenamiento interno o primario se hace en la memoria primaria[198]. Las computadoras utilizan dos clases de memoria primaria: memorias de sólo lectura o ROM (del inglés *read-only memory*) y las memorias de acceso aleatorio o RAM (de *random access memory*). La ROM almacena ciertos programas e informaciones que necesita la computadora; estas instrucciones están grabadas permanentemente, por eso se les conoce como memoria no volátil ya que no se borra ni desaparece cuando se desconecta la electricidad. En cambio, la RAM es una memoria volátil, que se pierde cuando se desconecta el aparato (o se interrumpe el fluido eléctrico)

El almacenamiento externo o secundario se realiza en dispositivos externos, entre los cuales los más utilizados son los discos. Por las indudables ventajas que presenta, los ingenieros han optado por

[198] Es la que contiene el sistema operativo, las instrucciones para manipular datos y los datos mismos.

desarrollar métodos de almacenamiento en discos, que al girar a velocidades altísimas pueden recuperar información más fácil que en dispositivos de cualquier otra forma geométrica. Los dispositivos externos tienen memoria ROM y entre ellos podemos señalar los discos duros, los discos suaves o disquetes, los discos compactos ROM; también las cintas pero ya prácticamente, salvo en grandes computadores, no se usan y se consideran obsoletas.

Cada documento constituye un **archivo informático**, que se procesa en el microprocesador y se puede guardar en dispositivos de memoria auxiliar para su posterior consulta y recuperación.

Lectura y escritura informática[199]

Es importante señalar que en Informática el proceso de transferencia de datos a un equipo de cómputo se conoce como procedimiento de **lectura.** Así, por ejemplo, cuando se digitan datos desde el teclado, cuando se capturan textos o imágenes desde un rastreador (*escáner*) o cuando se transfiere información desde un disquete o un disco compacto, se dice que el computador "está leyendo".

El proceso de transferencia desde el procesador hacia el almacenamiento secundario se denomina **procedimiento de escritura,** o sea el grabar la información; puede hacerlo en cintas, disquetes o discos compactos.

Otro aspecto que hay que indicar es el de que una computadora realiza todas sus operaciones en notación binaria (unos y ceros), en donde uno (1) significa activado y cero (0) desactivado; este sistema es similar a la naturaleza de encendido-apagado de los dispositivos eléctricos. El sistema binario permite representar números, letras del alfabeto y símbolos y realizar operaciones aritméticas de la misma forma en que las personas utilizan un sistema decimal o bien escriben un texto.

[199] Datos tomados básicamente de "Introducción a la Informática", de Tim Duffy, Grupo Editorial Iberoamérica, México, 1993, Ps. 50 y ss.

Ahora bien, para grabar (o "escribir"*)* se utilizan básicamente dos clases de discos: los magnéticos y los ópticos o compactos (CD).

Los discos magnéticos

Utilizan la tecnología de magnetización, que ha sido la tradicional y que consiste en almacenar impulsos magnéticos en superficies recubiertas con una capa finísima de óxido de hierro, que imantada produce la combinación binaria de magnetización[200] o desmagnetización. Los dispositivos pueden ser rígidos, como los discos duros, o flexibles como los disquetes (así como también las cintas).

Los discos compactos

Utilizan la tecnología **óptica**, que se vale del rayo láser - y no de la magnetización - para el registro y lectura de datos. Es un sistema de almacenamiento de información en el que la superficie del disco está recubierta de un material que refleja la luz.

La grabación de los datos se realiza creando agujeros o burbujas microscópicas que dispersan la luz (*pits)* alternándolos con zonas que sí la reflejan *(lands)*; se utiliza un rayo laser y un fotodiodo para leer esta información[201]. Se ha estudiado una codificación que permite llegar a cualquier dato, a partir de los *pits* y los *lands*, que están organizados en espiral, y no en círculos concéntricos (como en los disquetes). La luz es disparada constantemente contra el disco; si se topa con el *land* es reflejada; si, en cambio, da con un *pit* se dispersa. En consecuencia se produce una alternativa binaria en las condiciones, equivalente a la situación de magnetización o desmagnetización, propia de los soportes magnéticos.

[200] Magnetizada equivale a *activada* en lenguaje binario, o sea igual a uno; y desmagnetizada a *desactivada*, o sea igual a cero.
[201] Tomado de Enciclopedia ENCARTA 98, de Microsoft (en CD-ROM)

Para proveer mayores garantías a la recuperación de los errores se han desarrollado técnicas que hacen que hoy se produzca un error cada mil billones de caracteres (prácticamente no hay error). Así la seguridad que ofrece el disco compacto es excepcional. Las informaciones sobre el disco compacto se escriben según esta pauta: para que cada error sea individualizable, el byte pasa a 14 bits en vez de los 8 bits. A cada byte clásico (de 8 bits) se le agregan 6 bits de control.[202]

Las soluciones mediante el procesamiento de imágenes están construidas aprovechando la capacidad de convertir grandes volúmenes de información, contenida en papel, a formas electrónicas o "imágenes" que pueden ser almacenadas y accesadas por una computadora. Por primera vez, las organizaciones pueden manejar la información que se origina en un papel utilizando los mismos sistemas de información computarizados que manejan datos, textos, gráficas y voz. El resultado es un sistema de información con una base de datos y de textos que es accesible para mucha gente en forma simultánea rápida y fácil.[203]

CONCEPTO DE DOCUMENTO

Documento contenido y documento continente

Una primera distinción tenemos que hacer entre lo que podemos llamar **documento contenido**, que es "*lo escrito*" como reflejo de una constatación de hechos o de la expresión o acuerdo de voluntades. Tenemos por ejemplo una acta notarial, una acta de sesión de una junta directiva, un testamento, un contrato, etc. Y lo que podemos denominar **documento continente** que correspondería al elemento material en que se asienta el contenido. Los archivistas le denominan soporte.

---

[202] Mario Losano, "De la pluma de ganso al rayo láser", en "Informática y derecho- Aportes de doctrina Internacional", Volumen 2, Ed. Depalma, Bs. Aires, 1992.

[203] Los principales estándares utilizados para almacenar en este tipo de discos son el CD-ROM, CD-R o WORM, CD-DA, CD-I y PhotoD.

En primer término podemos observar una correspondencia de número entre los documentos manuales o impresos con el soporte papel (continente) y por el contrario, la enorme desproporción de los soportes electrónicos cuya capacidad de almacenamiento permite almacenar miles y millones de documentos en un solo disco compacto pequeño.

Otro aspecto que hay que señalar es la diferencia entre archivos digitados y archivos digitalizados. En los primeros cuando se "lee informáticamente" cualquier carácter tecleado se traduce instantáneamente a una combinación de dígitos binarios, llamada equivalente binario. El código binario determina cómo debe representarse en tal código cualquier carácter. La mayoría de las computadoras utilizan como código para representar datos el ASCII[204] (se pronuncia aski). Hay que notar que las letras mayúsculas y minúsculas tienen códigos distintos (p.e. la "A" de la "a"). En estos archivos se pueden hacer búsquedas de un carácter o una serie de caracteres, tales como de una letra o una palabra o una oración.

En los segundos, o sea los archivos digitalizados, lo que se ingresa o lee es una imagen[205], que puede contener un dibujo, una fotografía o un texto. El proceso de convertir la imagen contenida en papel en un archivo, se realiza por medio de un dispositivo llamado digitalizador. Los digitalizadores de alta resolución (400 o más puntos por pulgada cuadrada), se parecen y funcionan en forma similar a una fotocopiadora. Crean imágenes digitales (legibles para una computadora) que mantienen todas las características del documento original, incluyendo firmas, notas manuscritas, membretes, sellos, gráficas y fotografías. Una vez que el documento es digitalizado, el usuario crea índices de los archivos de imágenes con palabras clave, de tal modo que las imágenes pueden ser añadidas (como un gráfico) a la base de datos documental. Estas palabras clave serán utilizadas para la búsqueda dentro de la base de datos y la subsecuente recuperación del documento requerido.

---

[204] Acrónimo de American Standard Code for Information Interchange, o sea Código Americano Estándar para Intercambio de Información.

[205] Lógicamente también puede incluir voz o sonido, pero para no distraer el hilo conductor de la exposición lo circunscribimos a imágenes únicamente.

Los archivos de imágenes creados por el sistema, son comprimidos informáticamente para ahorrar espacio de almacenamiento en disco, pero aún así las imágenes altamente comprimidas utilizan grandes cantidades de espacio de almacenamiento en comparación con el espacio utilizado por los registros de datos tradicionales, como textos y números).

Ahora bien, estas imágenes son inertes o estáticas en el sentido de que, por ejemplo tratándose de textos, en ellas no pueden hacerse búsquedas puntuales como en el caso de los archivos digitados en que se pude localizar una palabra, una frase, una cadena de caracteres, etc. Para ello, es preciso convertir los textos digitalizados (imágenes) en textos digitados, por medio de la conversión de los textos a ASCII, mediante un tipo de software de reconocimiento óptico de caracteres (OCR).

Definiciones de documento

La distinción inicial que haremos es entre lo que podemos denominar "*documentos en sentido estricto"* de los "*documentos en sentido amplio*". Para los primeros, tenemos la definición de documento que nos la da el Diccionario de la Real Academia Española (tercera acepción), como *"... Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo."* Destacan en ella los siguientes elementos fundamentales: a) el de asiento material (escrito); b) que contiene datos fidedignos; y c) que pueden servir como prueba.

En un sentido parecido para Couture documento "es un

instrumento, objeto normalmente escrito, en cuyo texto se consigna o

representa alguna cosa apta para esclarecer un hecho o se deja constancia de una declaración de voluntad que produce efectos jurídicos"[206]

La segunda distinción, o sea los documentos en sentido amplio, encuentran apoyo en la doctrina contemporánea, como es el caso de Chiovenda[207] que en forma sintética pero completa define conceptualmente al documento:

> "*En un sentido amplio**, documento** es toda representación material destinada e idónea a reproducir una determinada manifestación de pensamiento"*.

Las mismas características que la anterior pero más sintética aún es la definición de Carnelutti:

> *"Documento es una cosa que sirve para conocer un hecho"*

De estas definiciones podemos destacar tres características del documento:

a) cualquier representación material, es decir una cosa o bien mueble;
b) que tenga como fin el de reproducir o representar algo, un hecho o un acto jurídico; y
c) que esté calificado para tal fin o sea su idoneidad.

[206] Eduardo J. Couture. Vocabulario Jurídico. Facultad de Derecho y Ciencias Sociales. Montevideo, 1950.
[207] Giusseppe Chiovenda, Instituciones de Derecho Procesal Civil, Vol. III, Ed. Revista de Derecho Privado, Madrid, 1954, p. 265

Evolución del concepto de documento en nuestro derecho positivo

A pesar de su importancia, nuestro legislador en vez de una definición puntual lo que ha establecido es una lista de elementos que deben o pueden ser considerados como documentos. Ahora bien, no se ha tratado de listas cerradas (*numerus clausus*) sino por el contrario, de elencos absolutamente abiertos, tal como se puede observar cronológicamente en las siguientes cuatro leyes que durante la última década han tratado sobre el tema.

El Código Procesal Civil, Ley Nº 7130 de 16 de octubre de 1989, en su artículo 368 nos da el siguiente elenco:

> *ARTICULO 368.- Distintas clases de documentos.*
> *Son documentos los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y, en general, todo objeto mueble que tenga carácter representativo o declarativo.*

El documento así concebido puede ser representativo, por cuanto está destinado a representar en el tiempo un hecho; o declarativo, cuando está destinado a plasmar una declaración de voluntad.

La Ley del Sistema Nacional de Archivos, Nº 7202 de 24 de octubre de 1990 establece:

> *"Artículo 3.- Todos los documentos con valor científico-cultural son bienes muebles y forman parte del patrimonio científico-*

cultural de Costa Rica. La determinación del valor científico - cultural del documento corresponderá a la Comisión Nacional de Selección y Eliminación de Documentos.

Se consideran de valor científico-cultural aquellos documentos textuales, manuscritos o impresos, gráficos, audiovisuales y legibles por máquina que, por su contenido, sirvan como testimonio y reflejen el desarrollo de la realidad costarricense, tales como: actas, acuerdos, cartas, decretos, informes, leyes, resoluciones, mapas, planos, carteles, fotografías, filmes, grabaciones, cintas magnéticas, "diskettes", y los demás que se señalen en el reglamento de esta ley."

La Ley de registro, secuestro y examen de documentos privados e intervención de las comunicaciones, Nº 7425 de 9 de agosto de 1994, define en su primer artículo:

"ARTICULO 1.- Competencia.

Los Tribunales de Justicia podrán autorizar el registro, el secuestro o el examen de cualquier documento privado, cuando sea absolutamente indispensable para esclarecer asuntos penales sometidos a su conocimiento.

Para los efectos de esta Ley, se consideran documentos privados: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros,

> los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representantivo o declarativo, para ilustrar o comprobar algo."

La Ley Orgánica del Poder Judicial con la reforma introducida por la Ley Nº 7728 de 15 de diciembre de 1997 que le adicionó el artículo 6 bis indica:

> "Artículo 6 bis.- Tendrán la validez y eficacia de un documento físico original, los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos o producidos por nuevas tecnologías, destinados a la tramitación judicial, ya sea que contengan actos o resoluciones judiciales. Lo anterior siempre que cumplan con los procedimientos establecidos para garantizar su autenticidad, integridad y seguridad. ..."

Estas cuatro leyes evidencian el intento de nuestro derecho positivo por el cambio tecnológico durante la última década e ir incorporando el nuevo instrumental documental. Se toma partido por una concepción de documento en sentido amplio. Las primeras tres lo hacen con una lista de los "inventos" o nuevos productos conforme van apareciendo y popularizándose en el mercado. En 1989 (Ley 7130) recoge todas las cosas que pueden constituir documentos, cuyas novedades son las fotocopias, los discos y las cintas magnetofónicas; en 1990 (Ley 7202) incorpora los disquetes; en 1994 adiciona los videos y los casetes. Pero, sin embargo, hay que reiterar que siempre mantiene una apertura hacia otros elementos que contengan características de reproducción o representación similares a las enlistadas, o bien deja su eventual incorporación al reglamento. En 1997 se abandona el modelo de lista (que dado el continuo adelanto tecnológico siempre resulta insuficiente) por una descripción de todos los medios posibles de recuperación y almacenamiento de información.

Otro aspecto que refuerza el argumento anterior es la aparición del fenómeno de la multimedia. El estudioso del tema, profesor López Garrido, en su obra " La crisis de las telecomunicaciones"[208], expone de manera elocuente la cuestión:

> *El fenómeno de la electrónica en este último cuarto de siglo ha revolucionado el mundo y nuestras vidas. La electrónica, entendiendo por tal el conjunto de técnicas que utilizan las variaciones de las magnitudes eléctricas para captar, trasmitir y*

[208] Ver "La crisis de las telecomunicaciones: el fenómeno desregulador en Estados Unidos, Japón y Europa", FUNDESCO, Comprint S.A, Madrid, 1989.

difundir una información, ha sido hasta hace poco limitada en su desarrollo.

Ello por dos tipos de razones: porque se trataba de técnicas caras y porque esas técnicas se aplicaban ***de manera diferente*** *a los diversos tipos de informaciones. Por ejemplo, en el caso de la informática se utilizaban informaciones numéricas) o alfanuméricas); en el caso de telecomunicaciones se utilizaba informaciones de sonido (voz, p.e.); y de imágenes como en el caso de las comunicaciones audiovisuales (videos).*

Los sectores de la electrónica se encontraban, por tanto, separados y bloqueados en su desarrollo. Esta situación ha recibido el impacto de una evolución tecnológica que ha transformado todas las actividades que tienen que ver con manipulación de la información.

Se trata de la ***numerización o digitalización de la información****, que permite tratar imágenes, cifras, textos escritos y sonidos de manera perfectamente homogénea. Las informaciones de cualquier naturaleza pueden ser tratadas* ***de manera similar.”*** (el destacado no es del original).

Una computadora, un aparato de televisión, un equipo de sonido, una central telefónica, un teléfono celular y una cámara fotográfica funcionan (o pueden funcionar) según principios parecidos. Es en una palabra la **multimedia**, en que se presenta la información utilizando una combinación de medios como sonido, gráficos, animación, vídeo y texto.

Corresponde a continuación emprender el análisis del documento electrónico.

El documento electrónico

Como describimos en la Introducción, existe actualmente una infinidad de tipos de documentación producida por medio del computador. Hay documentos que percibimos con nuestra vista en forma impresa y otros en las pantallas (o monitores) de equipos informáticos, los primeros constituyen comprobantes físicos del hecho o acto, en cambio en los otros vemos un reflejo de lo que queda registrado en archivos lógicos del equipo.

Giannantonio ha definido a aquellos documentos que son confeccionados por el computador por medio de sus periféricos de salida como ***documentos electrónicos en sentido amplio***[209]. Por nuestra parte[210], habíamos denominado como "*documento producido electrónicamente*" aquel que se imprime en papel o cualquier otro soporte duro (p.e. cerámica, plástico, vidrio, etc.), perceptible por el ojo humano y grabado por medios electrónicos (desde máquinas de escribir electrónicas, fax hasta impresoras laser).

Por otra parte, aquel documento grabado en un soporte magnético u óptico, legible únicamente con el auxilio de una máquina traductora o intérprete, el autor italiano lo ha denominado como ***documentos electrónicos en sentido estricto***[211] y a su vez los divide en dos tipos, de acuerdo con su perdurabilidad: aquellos cuyos datos se elaboran en las memorias primarias RAM, que son de carácter volátil, efímero (prácticamente son documentos instantáneos). o sea que se pierden automáticamente cuando se apaga el computador. Los otros, en cambio, tales como los datos contenidos en cintas o en discos magnéticos duros o flexibles, o bien en los discos con memorias magnético-ópticas (MOM) que permanecen memorizados hasta el momento en que una intervención humana proceda a cancelarlos o modificarlos. Entre éstos se incluyen los discos ópticos (CD-ROM), que están destinados a permanecer inalterables en el tiempo (una vez "quemado" el disco, no puede modificarse).

Giannantonio al concebir la escritura como la fijación sobre un soporte material de mensaje destinado a la conservación, afirma que no hay inconveniente para considerar el documento electrónico, como documento escrito, ya que:

1. Contiene un mensaje (texto alfanumérico o diseño gráfico).
2. Esta escrito en lenguaje convencional (el de los bits)[212].
3. Está sentado sobre soporte material (disco); y
4. Está destinado a durar en el tiempo.

En relación con los criterios de seguridad que permiten al documento electrónico constituirse en documento, Yves Poullet[213] ha señalado los siguientes:

- Debe ser inalterable;
- debe ser legible mediante un procedimiento adecuado;

---

[209] . Ettore Giannantonio, "El valor jurídico del documento electrónico" en Informática y Derecho Aportes de doctrina internacional, Volumen I, Ed. Depalma, Bs. Aires, 1991, p. 98.

[210] Ponencia "Valor jurídico del documento electrónico", en Reunión de expertos en Informática Jurídica de los países hispano-luso-americanos, Lisboa, Portugal, Noviembre 1993.

[211] Nosotros lo denominamos "documento electrónico propiamente dicho" .

[212] Agrego que sería más preciso decir en ASCII.

[213] Citado por V. Carrascosa L. "El documento eléctrónico on informático", en Revista de Informática y Derecho (dossier de la UNED de Mérida, España, 1995)

- debe ser identificado respecto al lugar (nombre y dirección) y al tiempo (fecha de redacción, de envío y de recepción); y
- debe ser estable, lo que plantea el problema del soporte físico y los métodos del rejuvenecimiento del soporte.

En la misma línea Rocco Borghini[214] afirma que el documento electrónico puede equipararse al documento en papel, pues cumple los tres requisitos fundamentales de todo documento: legibilidad, inalterabilidad y reconocimiento.

La autenticidad del documento electrónico

En cuanto a la autenticidad del documento o seguridad de su autoría, existen distintas técnicas capaces de otorgar certeza al documento electrónico[215]:

1) Utilización de códigos de usuario y de palabras clave (passwords) identificatorias. Estos procedimientos dependen de una combinación de caracteres alfanuméricos que es conocida sólo por el titular y que, además, puede ser modificado por éste con suma facilidad
2) Transmisión de textos encriptados o codificados de tal manera que los convierten en indescifrables para terceras personas.
3) Identificación del operador a través de características biométricas (por ejemplo, el iris del globo ocular, o la huella digital), fisiológicas (el registro de la voz) o personales de otro tipo (por ejemplo, reconocimiento por la computadora de la firma)[216].

.

Tales técnicas, aún en el estado actual de su desarrollo, proporcionan al documento un grado de certeza mayor que el que otorga

[214] Idem.
[215] Ver Giannantonio, op. cit.
[216] Sin embargo, existen programas que, sobre la base de la memorización de varias firmas auténticas, son capaces de estampar algo que podríamos llamar "una firma promedio" de las memorizadas, otorgándoles así a tal firma no escrita por su titular, un carácter de autenticidad superior a la propia firma del mismo, efectuada por ejemplo en momentos de nerviosismo, apuro o incomodidad.

hoy el examen caligráfico a la autenticidad del documento escrito. Es decir, la firma escrita "de puño y letra" es menos segura que la firma digital. Existe, naturalmente, una diferencia de costos; pero es preciso recordar que el uso creciente y generalizado del documento electrónico está intensificando las inversiones o investigaciones tendientes a diseñar dispositivos de seguridad que rodeen de certidumbre la manera en que se autentica o rubrica un documento. Es, pues el tema de las firmas, la digital y la digitalizada.

La firma digital

A continuación estudiaremos los aspectos fundamentales de la llamada firma digital, porque dado el auge del comercio internacional utilizando el correo electrónico, debido a la implantación de INTERNET, se considera que la firma digital es uno de los medios de promover un intercambio de bienes y servicios en forma ágil y consecuente con el medio.

Las empresas de la industria informática han desarrollado ingeniosos métodos para encriptar la información delicada que se comunica mediante redes públicas, utilizando la criptografía de llave pública[217].

La confidencialidad se obtiene mediante la encriptación del texto que hace el remitente de los mensajes para que sólo el destinatario programado pueda descifrarlo. En un sistema de llave pública, el remitente puede encriptar un mensaje con la llave pública del destinatario. Una vez encriptado, el mensaje sólo puede ser descifrado con la llave privada correspondiente. Puesto que sólo el destinatario tiene acceso a su llave privada, el remitente puede tener la seguridad de que nadie más puede descifrar el mensaje. La criptografía de llave pública

[217] La explicación de este novedoso tema la hemos tomado del artículo " Las autoridades de certificación y el comercio electrónico", de David Klur, de IS Audit &Control Journal, Vol. VI, 1996, ps. 28 a 33, bajado de INTERNET.

tambien puede ser usada para dar integridad a un mensaje mediante las firmas digitales.

Una firma digital se crea corriendo el texto del mensaje a través de un mecanismo lógico del sistema que produce un "resumen del mensaje", el que se encripta con la llave privada del remitente. A su vez, el receptor del mensaje descifra la firma digital con la llave pública del remitente y recalcula el resumen del mensaje. Si el nuevo resumen del mensaje calculado es igual al que se encontró en la firma, el mensaje no ha sido manipulado. Además, puesto que el resumen del mensaje fue encriptado con la llave privada que sólo el remitente conoce, este proceso asegura que el signatario del documento no puede desconocerlo posteriormente diciendo que la firma fue falsificada (esto se llama "no repudio").

Sin embargo, las firmas digitales no pueden por sí mismas brindar pruebas acerca de la identidad del remitente. Una forma de verificar las identidades digitales es por medio de terceros, en quienes se tenga confianza y actúen de manera independiente, realicen una verificación o certificación de las identidades. Son conocidos como "autoridades de certificación", en tanto que los documentos digitales emitidos por ellas se denominan "certificados".

Los certificados digitales ligan una identidad con un par de llaves criptográficas usadas para fines de encriptación y firma digital. Tales certificados permiten verificar la afirmación de que una llave pública determinada pertenece a un individuo determinado, y ayudan a evitar que alguien use una llave falsa para hacerse pasar por otra persona. Los certificados contienen una llave pública y un nombre, fecha de expiración, el nombre de la autoridad certificadora y lo más importante, la firma digital de la entidad emisora.[218]

Para el uso de la firma digital se requiere, además de los procedimientos arriba descritos, un acuerdo escrito inicial entre cada persona autorizada para usar las firmas digitales, en el que se definen los procedimientos y protocolos que utilizarán las partes para conducir una

[218] El formato más ampliamente aceptado se define en la norma internacional CCITT X.509.

serie de transacciones en el futuro, así como un medio y un procedimiento aceptados para registrar los elementos de esas transacciones. En dicho convenio las partes deben especificar una jurisdicción particular dentro de la cual regirá el mismo y de que están de acuerdo en que el concepto de firmas digitales es criptográficamente correcto.[219]

En los Estados Unidos también se está incrementando su uso a nivel gubernamental y para ello se ha dictado legislación específica; para regular la DSS (Digital Signature Standard, o sea Norma o Estándar de la Firma Digital) existe un órgano denominado Instituto Nacional de Normas y Tecnología (NIST, National Institute of Standarrds and Technology), que publica las Normas Federales sobre Procesamiento de Información (FIPS), o sea los estándares y lineamientos adoptados y promulgados con base en las disposiciones de la Sección III (d) de la Ley sobre la Propiedad Federal y los Servicios Administrativos, según fue modificada por la Ley sobre Seguridad Informática de 1987 (Ley Pública 110-235). Esta normativa ha asignado importantes responsabilidades a la Secretaría de Comercio y al NIST en cuanto se refiere al uso y administración de las computadoras y los sistemas de telecomunicaciones que emplea el gobierno federal norteamericano.

En conclusión podemos colegir que dado que la firma digital funciona dentro de círculos de correspondencia de signatarios que emiten y aceptan como firmas las combinaciones de caracteres que las constituyen y que aceptan la constatación de una autoridad certificadora superior, su reconocimiento con valor jurídico en nuestro medio no es posible, dado que la regulación misma como el establecimiento de las autoridades certificadoras correspondientes deben ser creadas por ley.

La firma digitalizada

La firma digitalizada es aquella que se escribe informáticamente hablando, o mejor dicho, se dibuja, en un dispositivo que permite estampar una rúbrica al igual que en un soporte papel, generando una imagen o gráfico que se incorpora al archivo del documento. Se trata de un lector óptico que consiste en una pantalla con sensores que reproducen los rasgos de la firma hecha con puño y letra. Un ejemplo de esta técnica es la utilizada para estampar la firma por el Tribunal Supremo de Elecciones en la emisión de la nueva presentación de la cédula de identidad.

Se trata de un documento jurídico electrónico en sentido estricto, pues es un archivo electrónico que sólo podemos percibir mediante el uso de un computador. No se puede confundir con un documento jurídico en sentido amplio, como sería el documento impreso en una computadora, al cual se le ha calzado la firma con una pluma o lapicero (que luego

[219] Ver "Lineamientos para firmas digitales con base en la legislación modelo", por Larry Zanger y Lorijean G. Oei, 1995. Bajado de INTERNET.

puede, a su vez ser digitalizado creando una imagen del documento completo).

El valor probatorio del documento

Uno de los aspectos que plantea la consulta es el valor probatorio del documento electrónico, al igual que el documento no electrónico. Resulta preciso repasar algunas nociones fundamentales sobre medios y fuentes de prueba.

El documento puede cumplir diversas funciones; en primer término, de carácter sustancial, como requisito necesario para la existencia de un negocio jurídico determinado, como requisito *ad-solemnitaten.* Para Giannantonio el ordenamiento jurídico toma en consideración la actividad de la documentación a causa de su importancia social y dicta al respecto su disciplina bajo diversos perfiles.

> *"Por sobre todo, disciplina las varias especies de documentos, su forma, su eficacia como medio de prueba y, a veces, como condición de validez de los actos jurídicos; mediante las normas penales prevé y pena los delitos de adulteración y tutela la fe pública, o sea la confianza de cada uno en la genuinidad, autenticidad y veracidad de los documentos y, por tanto, en su eficacia*[220]*."*

La segunda función es de carácter probatorio, cuando sirve o puede servir eventualmente de elemento de corroboración ante un conflicto de intereses; constituye uno de los aspectos más importantes, desde la óptica procesal, estudiar el carácter probatorio del documento. Lo primero que corresponde es, siguiendo la explicación de Heliè que retoma Sentís Melendo, repasar la genial distinción que Carnelutti hizo entre **fuentes y medios de prueba.** (En "La Prueba", de S. Sentís Melendo, Ed. EJEA, Bs. Aires, 1979, ps. 14 y ss.)

[220] Giannantonio, op. cit. Pág. 99.

Para una mejor comprensión de diferenciar entre fuentes y medios de prueba, Carnelutti parte de que hay que distinguir entre el perito y el testigo: o sea en el hecho de que el testigo existe antes del proceso; en cambio, al perito lo crea el proceso; el testigo existe no sólo antes, sino con total independencia del proceso y aunque éste no llegue a producirse.

El juez le da un encargo al perito para que realice un servicio; en cambio, el concepto de encargo no sirve, no funciona, respecto del testigo. Por ello, como todos sabemos, es que los peritos son medios de prueba fungibles que están a disposición del juez y que éste selecciona a discreción, en contraste con los testigos, cuyo número y personas vienen determinados por acontecimientos preprocesales y que han de tener una relación histórica con el asunto de que se trate. A propósito, según López Mesa-Valente[221] los testigos, "*no son otra cosa que una* ***memoria con soporte biológico*** *de donde se extraen representaciones o descripciones de hechos pasados*".

Como antes lo indicamos, para Carnelutti el documento es definido como "*una cosa que sirve para conocer un hecho*" en contraposición al testigo, que es una persona que narra, y no una cosa que representa.

Fuentes son los elementos probatorios que existen antes del proceso y con independencia de éste: así, **no sólo el documento** sino también el testigo; y, sobre todo, la cosa litigiosa; y el litigante, en cuanto sabe lo que ha ocurrido; pero no el perito, ni el reconocimiento judicial, ni la declaración del testigo o la de la parte. No deben confundirse, y ello es importante, con las pruebas preconstituidas.

Por otra parte, medios son las actuaciones judiciales con las cuales las fuentes se incorporan al proceso. Y así, el testigo es una fuente y su declaración es un medio. Tambien la parte -y lo que ella sabe- es una fuente y su reconocimiento por el juez es un medio. Lo mismo ha de decirse cuando se trate del examen pericial.

[221] Citado en Manual de Informática Jurídica, de Guibourg, Allende y Campanella, Ed. ASTREA, Bs. Aires, 1996, p. 235).

Igual distinción cabe hacer en cuanto a los documentos; éstos son **fuente**, independientemente de su carácter de prueba preconstituida; pero **su incorporación**, con todas las diligencias a que pueda dar lugar es el **medio**.

Las regulaciones archivísticas

Existe una serie de normas en el ordenamiento jurídico para la conservación de los documentos de particular importancia y para llevar los archivos apropiados; se trata de normas extraídas sustancialmente de las reglas de la ciencia de la archivística[222].

La decisión que llegue a tomar el Archivo Nacional respecto de la adopción o incorporación del disco compacto tanto como documento en sí como de copia de otros documentos, constituirá una de las más trascendentales de su existencia. Para ello deberá tomar todas las previsiones del caso, con el fin de que los documentos tengan el valor jurídico de fuente y eventualmente puedan constituirse en medio de prueba.

La Ley del Sistema Nacional de Archivos, Nº 7202 de 24 de octubre de 1990, establece en su artículo 11 las funciones que corresponden a la Junta Administrativa del Archivo Nacional en su carácter de máxima autoridad del Sistema Nacional de Archivos.

Al respecto son de particular interés las disposiciones contenidas en las incisos e, f y h de dicho artículo:

d) establecer las políticas archivísticas del país y recomendar estrategias para un adecuado desarrollo del Sistema Nacional de Archivos.
e) Formular recomendaciones técnicas sobre la producción y la gestión de documentos.

[222] Giannantonio, idem..

h) Formular recomendaciones técnicas sobre la administración de documentos producidos por medios automáticos.

Como se puede colegir de lo anterior, estas funciones trascienden el ámbito de la Institución, para normar una actividad a nivel nacional, como es el caso del establecimiento de las políticas archivísticas del país y la recomendación de estrategias para el adecuado desarrollo del Sistema Nacional de Archivos, igualmente la de recomendar para la producción y gestión de documentos, así como de los producidos por medios automáticos, léase documentos electrónicos.

Estas disposiciones "archivísticas" se potencian con las que observamos en los cuatro artículos arriba transcritos de nuestro derecho positivo, que autorizan por medio de la vía de reglamento establecer las que se requieren para establecer un adecuado ordenamiento respecto de la emisión, archivo y reproducción de documentos electrónicos.

CONCLUSION:

El disco compacto constituye un documento, tanto como continente como contenido, con valor jurídico, de conformidad con nuestro ordenamiento jurídico.

Corresponde al Archivo Nacional establecer las políticas y dictar las regulaciones específicas para permitir la recuperación y actualización de este instrumental tecnológico, que contemplen los requerimientos técnicos, archivísticos y administrativos, para que la producción de tal acervo pueda efectivamente cumplir y garantizar su función documental.

Atentamente,

Enrique Germán POCHET CABEZAS

Procurador – Director del SINALEVI

TARJETA

DISCO COMPACTO / VALOR PROBATORIO / DOCUMENTO/ DOCUMENTO ELECTRONICO

La Licda. Ana V. García de Benedictis, mediante oficio SD –6989 consulta sobre la validez del documento "escrito" en disco óptico (CD-ROM).

El Lic. Enrique G. Pochet Cabezas, mediante el Dictamen C-283-98 de 24 de diciembre de 1998 da respuesta a dicha consulta, realizando un análisis jurídico sobre temas afines a la cuestión, tales como el almacenamiento computarizado de la información, la lectura y escritura informática, los discos magnéticos y los compactos, el concepto de documento (continente y contenido), su definición, la evolución de documento en nuestro derecho positivo, el documento electrónico y su autenticidad, las firmas digital y digitalizada, el valor probatorio del documento, junto con las regulaciones archivísticas y la Ley del Archivo Nacional, concluyendo que el disco compacto constituye un documento, tanto como continente como contenido, con valor jurídico, de conformidad con nuestro ordenamiento jurídico.Corresponde al Archivo Nacional establecer las políticas y dictar las regulaciones específicas para permitir la recuperación y actualización de este instrumental tecnológico, que contemplen los requerimientos técnicos, archivísticos y administrativos, para que la producción de tal acervo pueda efectivamente cumplir y garantizar su función documental.

ANEXO 3

LEY MODELO DE LA CNUDMI SOBRE LAS FIRMA ELECTRÓNICAS

LEY MODELO DE LA CNUDMI SOBRE LAS FIRMAS ELECTRÓNICAS
2001

(Extracto del informe de la Comisión de las Naciones Unidas sobre el Derecho Mercantil Internacional sobre la labor de su trigésimo cuarto período de sesiones, celebrado en Viena, desde el 25 de junio al 13 de julio de 2001. El texto de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas fue adoptado el 5 de julio de 2001 [Nota: la versión final de la Guía para la incorporación al derecho interno de la Ley Modelo será publicada durante el segundo semestre del año 2001])

Anexo II

Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001)

Artículo 1

Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor.

* La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [Y] . "

** El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje (Afactoring@) ; arrendamiento con opción de compra (Aleasing@); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

Artículo 2

Definiciones

Para los fines de la presente Ley:
a) Por “firma electrónica” se entenderán 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 e indicar que el firmante aprueba la información recogida en el mensaje de datos;
b) Por “certificado” se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;
c) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;
d) Por “firmante” se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa;
e) Por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;
f) Por “parte que confía” se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.
Artículo 3
Igualdad de tratamiento de las tecnologías para la firma
Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.
Artículo 4
Interpretación
1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.
2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.
Artículo 5
Modificación mediante acuerdo
Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.
3 3
Artículo 6
Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.
2. El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.
3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:
a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.
4. Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:
a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o
b) aduzca pruebas de que una firma electrónica no es fiable.
5. Lo dispuesto en el presente artículo no será aplicable a: [Y].

Artículo 7
Cumplimiento de lo dispuesto en el artículo 6

1. [*La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia*] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.
2. La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8
Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:
a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;
b) sin dilación indebida, utilizar los medios que le proporcione el prestador

de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:
i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o
ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;
c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.
2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).
Artículo 9
Proceder del prestador de servicios de certificación
1. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:
a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;
b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;
c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:
i) la identidad del prestador de servicios de certificación;
ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;
iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;
d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:
i) el método utilizado para comprobar la identidad del firmante;
ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;
iii) si los datos de creación de la firma son válidos y no están en entredicho;
iv) cualquier limit ación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8 de la presente Ley;
vi) si se ofrece un servicio para revocar oportunamente el certificado;
e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que existe un servicio para revocar oportunamente el certificado;
f) utilizar, al pre star sus servicios, sistemas, procedimientos y recursos humanos fiables.
2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1).
Artículo 10
Fiabilidad
A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:
a) los recursos humanos y financieros, incluida la existencia de activos;
b) la calidad de los sistemas de equipo y programas informáticos;
c) los procedimientos para la tramitación del certificado y las solicit udes de certificados, y la conservación de registros;
d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;
e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente;
6
f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o
g) cualesquiera otros factores pertinentes.
Artículo 11
Proceder de la parte que confía en el certificado
Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:
a) verificar la fiabilidad de la firma electrónica; o
b) cuando la firma electrónica esté refrendada por un certificado:
i) verificar la validez, suspensión o revocación del certificado; y
ii) tener en cuenta cualquier limitación en relación con el certificado.
Artículo 12
Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:
a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.
2. Todo certificado expedido fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que todo certificado expedido en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.
3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.
4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2), o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.
5. Cuando, sin perjuicio de lo dispuesto en los párra fos 2), 3) y 4), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.

ANEXO 4

REAL DECRETO LEY 14/1999

Real Decreto Ley 14/1999,
de 17 de septiembre, sobre firma electrónica

El Estado español ha tenido una participación activa en el logro de la posición común que facilita la tramitación del texto, al recoger éste los elementos suficientes para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica. En ese sentido, existen ya en España diversas normas sobre la presentación de la declaración del Impuesto sobre la Renta de las Personas Físicas por medios telemáticos, dictadas por la Administración tributaria. La Comisión Nacional del Mercado de Valores, por su parte, ha aprobado y puesto en marcha un sistema de cifrado y firma electrónica que se emplea para la recepción de información de las entidades supervisadas. Asimismo, el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, anuncia la posibilidad de prestar, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de la emisión y recepción de comunicaciones, a través de técnicas y medios electrónicos, informáticos y telemáticos. La Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda actuará en colaboración con Correos y Telégrafos.

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

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

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

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

En su virtud, a propuesta del Ministro de Fomento, de la Ministra de Justicia y del Ministro de Industria y Energía, previo informe del Consejo General del Poder Judicial y de la Agencia de Protección de Datos, tras la deliberación del Consejo de Ministros, en su reunión

celebrada el día 17 de septiembre de 1999, y en uso de la autorización concedida en el artículo 86 de la Constitución,

DISPONGO:

TITULO PRIMERO

Disposiciones generales

CAPITULO UNICO

Artículo 1. Ámbito de aplicación.

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

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

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

Artículo 2. Definiciones.

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

a) "Firma electrónica": Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

b) "Firma electrónica avanzada": Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

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

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

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

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

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

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

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

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

k) "Prestador de servicios de certificación": Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

l) "Producto de firma electrónica": Es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma

electrónica por el prestador de servicios de certificación o para la creación o verificación de firma electrónica.

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

Artículo 3. Efectos jurídicos de la firma electrónica.

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

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

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

TITULO II

La prestación de servicios de certificación

CAPITULO PRIMERO

Principios generales

Artículo 4. Régimen de libre competencia.

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

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

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

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

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

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

2. Las condiciones adicionales a las que se refiere el apartado anterior deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o extranjeras.
3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

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

1. El Gobierno, por Real Decreto, podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica, determinando, para ello, un régimen que permita lograr el adecuado grado de seguridad y proteger, debidamente, los derechos de los usuarios.
2. Las funciones de certificación a las que se refiere este Real Decreto-ley serán ejercidas por los órganos, en cada caso competentes, referidos en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones; en la Ley 21/1992, de 16 de julio, de Industria, y en la demás legislación vigente sobre la materia. El Real Decreto al que se refiere el apartado 1 establecerá las condiciones que permitan coordinar los sistemas de certificación.
3. Las normas que regulen los sistemas de acreditación y de certificación deberán ser objetivas, razonables y no discriminatorias. Todos los prestadores de servicios que se sometan voluntariamente a ellos, podrán obtener la correspondiente acreditación de su actividad o, en su caso, la certificación del producto de firma electrónica que empleen.
4. Los órganos competentes para el ejercicio de las funciones a que se refiere el apartado anterior valorarán los informes técnicos que emitan las entidades de evaluación sobre los prestadores de servicios que hayan solicitado su acreditación o los productos para los que se haya pedido certificación. También tomarán en cuenta el cumplimiento, por el prestador de servicios, de los requisitos que se determinen reglamentariamente para poder ser acreditado.
5. A los efectos de este Real Decreto-ley, sólo podrán actuar como entidades de evaluación aquellas que hayan sido acreditadas por el organismo independiente al que se haya atribuido esta facultad por el Real Decreto al que se refiere el apartado primero de este artículo.

Artículo 7. Registro de Prestadores de Servicios de Certificación.

1. Se crea, en el Ministerio de Justicia, el Registro de Prestadores de Servicios de Certificación, en el que deberán solicitar su inscripción, con carácter previo al inicio de su actividad, todos los establecidos en España. Su regulación se desarrollará por Real Decreto.
2. La solicitud de inscripción habrá de formularse, aportando la documentación que se establezca reglamentariamente, a efectos de la identificación del prestador de servicios de certificación y de justificar que éste reúne los requisitos necesarios, en cada caso, para ejercer su actividad. También será objeto de inscripción ulterior cualquier circunstancia relevante, a efectos de este Real Decreto-ley, relativa al prestador de servicios de certificación, como su acreditación o estar en condiciones de expedir certificados reconocidos.

La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente.
3. El Registro de Prestadores de Servicios de Certificación será público y deberá mantener permanentemente actualizada y a disposición de cualquier persona una relación de los inscritos, en la que figurarán su nombre o razón social, la dirección de su página en Internet o de correo electrónico, los datos de verificación de su firma electrónica y, en su caso, su condición de acreditado o de tener la posibilidad de expedir certificados reconocidos. En la citada relación figurarán, también, cualesquiera otros datos complementarios que se determinen por Real Decreto.
Los datos inscritos en el Registro podrán ser consultados por vía telemática o a través de la oportuna certificación registral. El suministro de esta información podrá sujetarse al pago de una tasa, cuyos elementos esenciales se determinarán por ley.

CAPITULO II

Certificados

Artículo 8. Requisitos para la existencia de un certificado reconocido.
1. Los certificados reconocidos, definidos en el artículo 2 j) de este Real Decreto-ley, tendrán el siguiente contenido:
a) La indicación de que se expiden como tales.
b) El código identificativo único del certificado.
c) La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.
d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.
f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.
g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.
h) El comienzo y el fin del período de validez del certificado.
i) Los límites de uso del certificado, si se prevén.
j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.
2. La consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

Artículo 9. Vigencia de los certificados.
1. Los certificados de firma electrónica quedarán sin efecto, si concurre alguna de las siguientes circunstancias:
a) Expiración del período de validez del certificado.
Tratándose de certificados reconocidos, éste no podrá ser superior a cuatro años, contados desde la fecha en que se hayan expedido.

b) Revocación por el signatario, por la persona física o jurídica representada por éste o por un tercero autorizado.
c) Pérdida o inutilización por daños del soporte del certificado.
d) Utilización indebida por un tercero.
e) Resolución judicial o administrativa que lo ordene.
f) Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
g) Cese en su actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicios.
h) Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.
2. La pérdida de eficacia de los certificados, en los supuestos de expiración de su período de validez y de cese de actividad del prestador de servicios, tendrá lugar desde que estas circunstancias se produzcan. En los demás casos, la extinción de la eficacia de un certificado surtirá efectos desde la fecha en que el prestador de servicios tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en su Registro de certificados al que se refiere el artículo 11.e).
3. En cualquiera de los supuestos indicados, el prestador de servicios de certificación, habrá de publicar la extinción de eficacia del certificado en el Registro al que se refiere el artículo 11.e), y responderá de los posibles perjuicios que se causen al signatario o a terceros de buena fe, por el retraso en la publicación. Corresponderá al prestador de servicios la prueba de que los terceros conocían las circunstancias invalidantes del certificado.
4. El prestador de servicios de certificación podrá suspender, temporalmente, la eficacia de los certificados expedidos, si así lo solicita el signatario o sus representados o lo ordena una autoridad judicial o administrativa. La suspensión surtirá efectos en la forma prevista en los dos apartados anteriores.
Artículo 10. Equivalencia de certificados.
Los certificados que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro de la Unión Europea, de acuerdo con la legislación de éste, expidan como reconocidos, se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumplan alguna de las siguientes condiciones:
a) Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado, conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.
b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.
c) Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.
CAPITULO III
Condiciones exigibles a los prestadores de servicios de certificación
Artículo 11. Obligaciones de los prestadores de servicios de certificación.
Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:
a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los

certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho. Se exceptúan de esta obligación, los prestadores de servicios de certificación que, expidiendo certificados que no tengan la consideración de reconocidos, se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquéllos.
b) Poner a disposición del signatario los dispositivos de creación y de verificación de firma electrónica.
c) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite.
d) Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial.
e) Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o perdida de vigencia de sus efectos. A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario.
f) En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo con la antelación indicada en el apartado 1 del artículo 13, a los titulares de los certificados por ellos emitidos y, si estuvieran inscritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.
g) Solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación.
h) Cumplir las demás normas previstas, respecto de ellos, en este Real Decreto-ley y en sus normas de desarrollo.

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

Además de cumplir las obligaciones establecidas en los artículos 7 y 11, los prestadores de servicios de certificación que expidan certificados reconocidos, han de cumplir las siguientes:
a) Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.
b) Demostrar la fiabilidad necesaria de sus servicios.
c) Garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata.
d) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.
e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
f) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación.
g) Disponer de los recursos económicos suficientes para operar de conformidad con lo dispuesto en este Real Decreto-ley y, en particular, para afrontar el riesgo de la responsabilidad por daños y perjuicios. Para ello, habrán de garantizar su responsabilidad frente a los usuarios de sus servicios y terceros afectados por éstos. La garantía a constituir podrá consistir en un afianzamiento mercantil prestado por una entidad de crédito o en un seguro de caución.

Inicialmente, la garantía cubrirá, al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100.
En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe.
h) Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años. Esta actividad de registro podrá realizarse por medios electrónicos.
i) Antes de expedir un certificado, informar al solicitante sobre el precio y las condiciones precisas de utilización del certificado. Dicha información, deberá incluir posibles límites de uso, la acreditación del prestador de servicios y los procedimientos de reclamación y de resolución de litigios previstos en las leyes y deberá ser fácilmente comprensible. Estará también a disposición de terceros interesados y se incorporará a un documento que se entregará a quien lo solicite. Para comunicar esta información, podrán utilizarse medios electrónicos si el signatario o los terceros interesados lo admiten.
j) Utilizar sistemas fiables para almacenar certificados, de modo tal que:
1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas.
2. Unicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones.
3. Pueda comprobarse la autenticidad de la información.
4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.
k) Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir, respetando este Real Decreto-ley y sus disposiciones de desarrollo, en el ejercicio de su actividad.

Artículo 13. Cese de la actividad.

1. El prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos y transferir, con su consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.
2. Si el prestador de servicios estuviere inscrito en el Registro de Prestadores de Servicios de Certificación del Ministerio de Justicia, deberá comunicar a éste, con la antelación indicada en el anterior apartado, el cese de su actividad, y el destino que vaya a dar a los certificados especificando, en su caso, si los va a transferir y a quién o si los dejará sin efecto. Igualmente, indicará cualquier otra circunstancia relevante, que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de un procedimiento de quiebra o suspensión de pagos respecto de él.
3. La inscripción del prestador de servicios de certificación en el Registro de Prestadores de Servicios de Certificación será cancelada, de oficio, por el Ministerio de Justicia, cuando aquél cese en su actividad. El Ministerio de Justicia se hará cargo de la información relativa a los certificados que se hubieren dejado sin efecto por el prestador de servicios de certificación, a efectos de lo previsto en el artículo 12.h).

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

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone este Real Decreto-ley o actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.
2. El prestador de servicios de certificación sólo responderá de los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.
3. La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, con las especialidades previstas en este artículo. Cuando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros.
4. Lo dispuesto en este artículo, se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios.

Artículo 15. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación al que se refiere este Real Decreto-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.
2. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.
3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre. Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

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

CAPITULO IV

Inspección y control de la actividad de los prestadores de servicios de certificación

Artículo 16. Supervisión y control.

1. El Ministerio de Fomento controlará, a través de la Secretaría General de Comunicaciones, el cumplimiento, por los prestadores de servicios de certificación que expidan al público certificados reconocidos, de las obligaciones establecidas en este Real Decreto-ley y en sus disposiciones de desarrollo. Asimismo, vigilará el cumplimiento, por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones establecidas en el artículo 11.

2. En el ejercicio de su actividad de control, la Secretaría General de Comunicaciones actuará de oficio, mediante petición razonada del Ministerio de Justicia o de otros órganos administrativos o a instancia de persona interesada. Los funcionarios de la Secretaría General de Comunicaciones adscritos a la Inspección de las Telecomunicaciones, a efectos de cumplir las tareas de control, tendrán la consideración de autoridad pública.
3. Cuando, como consecuencia de una actuación inspectora, se tuviera constancia de la contravención en el tratamiento de datos, de lo dispuesto en el artículo 11.c), la Secretaría General de Comunicaciones pondrá el hecho en conocimiento de la Agencia de Protección de Datos. Esta podrá, con arreglo a la Ley Orgánica 5/1992, iniciar el oportuno procedimiento sancionador, con arreglo a la legislación que regula su actividad.

Artículo 17. Deber de colaboración.
Los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría General de Comunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, referida siempre a datos que conciernan al prestador de servicios.
Artículo 18. Resoluciones del órgano de supervisión.
La Secretaría General de Comunicaciones podrá ordenar a los prestadores de servicios de certificación la adopción de las medidas apropiadas para exigirles que cumplan este Real Decreto-ley y sus disposiciones de desarrollo.
TITULO III
Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable
CAPITULO UNICO
Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable
Artículo 19. Dispositivos seguros de creación de firma electrónica.
A efectos del artículo 2 f), para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:
1.º Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.
2.º Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.
3.º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.
4.º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Artículo 20. Normas técnicas.
1. Se presumirá que los productos de firma electrónica que se ajusten a las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de las Comunidades Europeas" son conformes con lo previsto en la letra e) del artículo 12 y en el artículo 19.
2. Sin perjuicio de esta presunción, los números de referencia de esas normas se publicarán en el "Boletín Oficial del Estado".

Artículo 21. Evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica.

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

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

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

Artículo 22. Dispositivos de verificación de firma.

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

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

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

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

4. Que se verifica de forma fiable el certificado.

5. Que puede detectarse cualquier cambio relativo a su seguridad.

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

TITULO IV

Tasa por el reconocimiento de acreditaciones y certificaciones

CAPITULO UNICO

Tasa por el reconocimiento de acreditaciones y certificaciones

Artículo 23. Régimen aplicable a la tasa.

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

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

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

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

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

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

TITULO V
Infracciones y sanciones
CAPITULO UNICO
Infracciones y sanciones

Artículo 24. Clasificación de las infracciones.
Las infracciones de las normas reguladoras de la firma electrónica y los servicios de certificación se clasifican en muy graves, graves y leves.
Artículo 25. Infracciones.
1. Son infracciones muy graves:
a) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h).
b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones impuestas en las letras c) a la j) del artículo 12, siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.
c) El incumplimiento grave y reiterado por los prestadores de servicios de certificación de las resoluciones dictadas por la Secretaría General de Comunicaciones, para asegurar el respeto a este Real Decreto-ley.
2. Son infracciones graves:
a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos, de las obligaciones impuestas en cualquiera de las letras del artículo 11, salvo la c), la g) y la h), siempre que se causen daños graves a los usuarios o a terceros o se afecte gravemente a la seguridad de los servicios de certificación.
b) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones previstas en las letras a), b), y k) del artículo 12.
c) El incumplimiento por los prestadores de servicios de certificación que expidan certificados reconocidos de las obligaciones contempladas en las letras c) a la j) del artículo 12, cuando no concurran las circunstancias previstas en el apartado 1.b) de este artículo.
d) La falta de comunicación por el prestador de servicios de certificación al Ministerio de Justicia, en los plazos previstos en el artículo 13, del cese de su actividad o de la iniciación, respecto de él, de un procedimiento de suspensión de pagos o de quiebra.
e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo, con arreglo a este Real Decreto-ley.
f) El incumplimiento de las resoluciones dictadas por la Secretaría General de Comunicaciones para asegurar que el prestador de servicios de certificación se ajuste a este Real Decreto-ley, cuando no deba considerarse como infracción muy grave, conforme al apartado 1.c) de este artículo.
3. Son infracciones leves:
a) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en cualquiera de las letras del artículo 11, excepto la c), cuando no deba considerarse como infracción grave, de acuerdo con lo previsto en el apartado 2 a) de este artículo.
b) La expedición de certificados reconocidos que incumplan alguno de los requisitos establecidos en el artículo 8.

c) No facilitar los datos requeridos, en el ámbito de sus respectivas funciones, por el Ministerio de Justicia o la Secretaría General de Comunicaciones para comprobar el cumplimiento de este Real Decreto-ley por los prestadores de servicios de certificación.
d) Cualquier otro incumplimiento de las obligaciones impuestas a los prestadores de servicios de certificación por este Real Decreto-ley, salvo el de la recogida en el artículo 11.c) o que deba ser considerado como infracción grave o muy grave, de acuerdo con lo dispuesto en los apartados anteriores.

Artículo 26. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:
a) Por la comisión de infracciones muy graves, se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 1 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 5 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 100.000.000 de pesetas (601.012,10 euros).
La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años. Cuando la resolución de imposición de esta sanción sea firme, será comunicada al Registro de Prestadores de Servicios de Certificación para que cancele la inscripción del prestador de servicios sancionado.
b) Por la comisión de infracciones graves, se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria. A estos efectos, se considerarán las siguientes cantidades: El 0,5 por 100 de los ingresos brutos anuales obtenidos por la entidad infractora en el último ejercicio o, en caso de inexistencia de éstos, en el ejercicio actual; el 2 por 100 de los fondos totales, propios o ajenos, utilizados para la comisión de la infracción o 50.000.000 de pesetas (300.506,04 euros).
c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 euros).
2. Las infracciones graves y muy graves podrán llevar aparejada la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional, una vez que aquélla tenga carácter firme.
3. La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, lo siguiente:
a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.
b) La repercusión social de las infracciones.
c) El daño causado, siempre que no haya sido tomado en consideración para calificar la infracción como leve, grave o muy grave.
d) El beneficio que haya reportado al infractor el hecho objeto de la infracción.
4. Se anotarán en el Registro de Prestadores de Servicios de Certificación las sanciones impuestas por resolución firme a éstos por la comisión de cualquier infracción grave o muy

grave. Las notas relativas a las sanciones se cancelarán una vez transcurridos los plazos de prescripción de las sanciones administrativas previstos en la Ley reguladora del procedimiento administrativo común.
5. Las cuantías señaladas en este artículo serán actualizadas periódicamente por el Gobierno, mediante Real Decreto, teniendo en cuenta la variación de los índices de precios al consumo.

Artículo 27. Medidas cautelares.
En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte. Estas medidas podrán consistir en la orden de cese temporal de la actividad del prestador de servicios de certificación, en la suspensión de la vigencia de los certificados por él expedidos o en la adopción de otras cautelas que se estimen precisas. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

Artículo 28. Procedimiento sancionador.
1. El ejercicio de la potestad sancionadora atribuida por este Real Decreto-ley corresponde a la Secretaría General de Comunicaciones del Ministerio de Fomento. Para ello, la Secretaría General de Comunicaciones se sujetará al procedimiento aplicable, con carácter general, al ejercicio de la potestad sancionadora por las Administraciones públicas.
2. El Ministerio de Justicia y los demás órganos que ejercen competencias con arreglo a este Real Decreto-ley y sus normas de desarrollo podrán instar la incoación de un procedimiento sancionador, mediante petición razonada dirigida a la Secretaría General de Comunicaciones

DISPOSICION TRANSITORIA UNICA

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

DISPOSICIONES FINALES

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

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

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

Dado en Madrid a 17 de septiembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSE MARIA AZNAR LOPEZ

ANEXO 5

LEY # 431 PANAMÁ

LEY No. 431 Panamá
De 31 de julio de 2001
Que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos
LA ASAMBLEA LEGISLATIVA
DECRETA:

Título I
Comercio Electrónico y Documentos Electrónicos en General
Capítulo I
Ámbito de Aplicación

Artículo 1. Regulación. La presente Ley regula los documentos y firmas electrónicas y la prestación de servicios de certificación de estas firmas, y el proceso voluntario de acreditación de prestadores de servicios de certificación, para su uso en actos o contratos celebrados por medio de documentos y firmas electrónicas, a través de medios electrónicos de comunicación.

Artículo 2. Definiciones. Para los efectos de la presente Ley, los siguientes términos se definen así:

1. *Certificado.* Manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas electrónicas o la integridad de un mensaje.
2. *Destinatario.* Persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a ese mensaje.
3. *Documento electrónico.* Toda representación electrónica que da testimonio de un hecho, una imagen o una idea.
4. *Entidad de certificación.* Persona que emite certificados electrónicos en relación con las firmas electrónicas de las personas, ofrece o facilita los servicios de

1 Publicada en la Gaceta Oficial No. 24.359 de 3 de agosto de 2001.

registro y estampado cronológico de la transmisión y recepción de mensajes de datos y realiza otras funciones relativas a las firmas electrónicas.
5. *Firma electrónica.* Todo sonido, símbolo o proceso electrónico vinculado a o lógicamente asociado con un mensaje, y otorgado o adoptado por una persona con la intención de firmar el mensaje que permite al receptor identificar a su autor.
6. *Iniciador.* Toda persona que, a 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 ese mensaje.
7. *Intermediario.* Toda persona que, actuando por cuenta de otra, envíe, reciba o archive un mensaje o preste algún otro servicio con respecto a él.
8. *Mensaje de datos.* Información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.
9. *Repositorio.* Sistema de información utilizado para guardar y recuperar certificados u otro tipo de información relevante para la expedición de éstos.
10. *Revocar un certificado.* Finalizar definitivamente el periodo de validez de un certificado, desde una fecha específica en adelante.

11. *Sistema de información.* Todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.
12. *Suscriptor.* Persona que contrata con una entidad de certificación la expedición de un certificado, para que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma electrónica.
13. *Suspender un certificado.* Interrumpir temporalmente el periodo operacional de un certificado, desde una fecha en adelante.
Artículo 3. Interpretación. Las actividades reguladas por esta Ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional, equivalencia del soporte electrónico al soporte de papel y equivalencia funcional del comercio tradicional con el comercio electrónico. Toda interpretación de los preceptos de esta Ley deberá guardar armonía con los principios señalados.
Ley No. 43 de 2001 2
Artículo 4. Modificación mediante acuerdo. Salvo que se disponga otra cosa, en las relaciones entre las partes que generan, envían, reciben, archivan o procesan de alguna u otra forma mensajes de datos, las disposiciones del Capítulo III, Título I, podrán ser modificadas mediante acuerdo. Lo dispuesto en este artículo no se aplicará a las disposiciones contenidas en el Capítulo II del Título I de la presente Ley.
Artículo 5. Reconocimiento jurídico de los mensajes de datos. Se reconocen efectos jurídicos, validez y fuerza obligatoria a todo tipo de información, que esté en forma de mensaje de datos o que figure simplemente en el mensaje de datos en forma de remisión.
CCaappíítuulloo IIII
AAppllicaacciióónn ddee lloss RReeqquuiissiittoos JJuurrííddiccoos aa lloos MMeennssaajeess ddee DDaattoos
Artículo 6. Escrito. Cuando la ley requiera que la información conste por escrito, los actos y contratos, otorgados o celebrados, por medio de documento electrónico, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que éstos consten por escrito, siempre que se cumplan las condiciones siguientes:
1. Que la información que éste contiene sea accesible para su posterior consulta.
2. Que el mensaje de datos sea conservado con el formato original en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida.
3. Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, la fecha y la hora en que fue enviado o recibido.
Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.
Lo dispuesto en el presente artículo no será aplicable a:
1. Los actos para los cuales la ley exige una solemnidad que no sea verificable mediante documento electrónico.
2. Los actos jurídicos para los que la ley requiera la concurrencia personal de alguna de las partes.
3. Los actos jurídicos relativos al Derecho de Familia.
Ley No. 43 de 2001 3

Artículo 7. Firma. Cuando la ley exija la presencia de una firma o establezca ciertas consecuencias en ausencia de ella, en relación con un documento electrónico o mensaje de datos, se entenderá satisfecho dicho requerimiento si éste ha sido firmado electrónicamente.
La firma electrónica, cualquiera que sea su naturaleza, será equivalente a la firma manuscrita para todos los efectos legales. En cuanto a su admisibilidad en juicio y al defecto probatorio de los documentos y firmas electrónicas se aplicará lo dispuesto en la presente Ley. Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.
Si una disposición legal requiere que una firma relacionada a un documento electrónico o mensaje de datos o una transacción sea notarizada, reconocida, refrendada o hecha bajo la gravedad del juramento, dicho requisito será satisfecho si la firma electrónica de la persona autorizada para efectuar dichos actos, junto con toda la información requerida bajo la norma legal aplicable, sea vinculada con la firma o mensaje.
Lo dispuesto en el presente artículo no será aplicable a:
1. Los contratos sobre bienes inmuebles y demás actos susceptibles de registro ubicados en Panamá.
2. Los actos en materia de sucesiones que se otorguen bajo ley panameña o que sufran sus efectos en Panamá.
3. Los avisos y documentos dirigidos o emitidos por autoridades de Panamá, que no hayan sido autorizados por la entidad respectiva.
Artículo 8. Original. Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:
1. Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma.
2. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.
Lo dispuesto en este artículo se aplicará tanto si el requisito en él previsto constituye una obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no conste en su forma original.
Ley No. 43 de 2001 4
Artículo 9. Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.
Artículo 10. Admisibilidad y fuerza probatoria de los documentos, firmas electrónicas y mensajes de datos. Los documentos y firmas electrónicas y mensajes de datos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Capítulo III, del Título VII del Libro Segundo de Procedimiento Civil del Código Judicial, de conformidad con lo que dispone la ley.
Artículo 11. Criterio para valorar probatoriamente los documentos electrónicos, firmas electrónicas y mensajes de datos. Para la valoración de la fuerza probatoria de los documentos electrónicos, las firmas electrónicas y de los mensajes de datos a que se refiere

esta Ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas.

Por consiguiente, al valorar la fuerza probatoria de un documento electrónico, firma electrónica o mensaje de datos se habrá de tener presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad de la forma en la se haya conservado la integridad de la información y la forma en la que se identifiquen a su iniciador y a cualquier otro factor pertinente.

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

1. Que la información que contenga sea accesible para su posterior consulta;
2. Que el mensaje de datos sea conservado en el formato en que se haya generado, enviado o recibido o con algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida; y
3. Que se conserve, de haber alguno, todo dato que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido.

Si un cambio en la configuración en el sistema de información requerido para consultar un mensaje de datos crea un riesgo material de que el consumidor no pueda acceder a él, el proveedor suministrará al consumidor una declaración de las nuevas configuraciones requeridas, así como la oportunidad de dar por terminado el contrato.

Ley No. 43 de 2001 5

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

Los libros y documentos del comerciante podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta. Esta obligación estará sujeta a la prescripción de toda acción que pudiera derivarse de ella, según lo establecido en el artículo 93 del Código de Comercio.

Artículo 13. Conservación de mensajes de datos y archivo de documentos a través de terceros. El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos, se podrá realizar a través de terceros, siempre que se cumplan las condiciones enunciadas en el artículo anterior, además de que estos datos no contengan información sensible a los intereses del usuario.

CAPÍTULO III

COMUNICACIÓN DE LOS MENSAJES DE DATOS Y DOCUMENTOS ELECTRÓNICOS

Artículo 14. Formación y validez de los contratos. En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. Se reconoce validez y fuerza obligatoria a un contrato que para su formación utilice uno o más mensajes de datos.

Artículo 15. Reconocimiento de los mensajes de datos por las partes. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, se reconocen efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración que conste en forma de mensaje de datos o documento electrónico.

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

1. El propio iniciador;

2. Alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o
3. Un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.

Artículo 17. Presunción del origen de un mensaje de datos. Se presume que un mensaje de datos ha sido enviado por el iniciador, y por lo tanto puede actuar en consecuencia, cuando:

Ley No. 43 de 2001 6

1. Haya aplicado en forma adecuada el procedimiento acordado previamente con el iniciador, con el fin de establecer que el mensaje de datos provenía efectivamente de éste; o
2. El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.

Parágrafo. Lo dispuesto en el presente artículo no se aplicará:

a. A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia; o
b. A partir del momento en que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o haber aplicado algún método convenido, que el mensaje de datos no provenía de éste.

Artículo 22. Concordancia del mensaje de datos enviado con el mensaje de datos recibido. Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, éste último tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia.

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

Artículo 23. Mensajes de datos duplicados. Se presume que cada mensaje de datos recibido es un mensaje de datos diferente, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el nuevo mensaje de datos era un duplicado.

Artículo 24. Acuse de recibo. Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

1. Toda comunicación del destinatario, automatizada o no; o
2. Todo acto del destinatario, que baste para indicar al iniciador que se ha recibido el mensaje de datos.

Ley No. 43 de 2001 7

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

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, pero aquél no indicó expresamente que los efectos del mensaje de datos están condicionados a la recepción del acuse de recibo y, si no se ha recibido acuse en el plazo fijado o convenido, o no se ha fijado o convenido ningún plazo, en un plazo no mayor de

cuarenta y ocho horas a partir del momento del envío o del vencimiento del plazo fijado o convenido, el iniciador:
a. Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un nuevo plazo para su recepción, el cual será de cuarenta y ocho horas, contado a partir del momento del envío del nuevo mensaje de datos; y
b. De no recibirse acuse de recibo dentro del término señalado conforme al literal anterior, podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.
Artículo 21. Presunción de recepción de un mensaje de datos. Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos.
Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido. Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.
Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.
Artículo 22. Tiempo del envío de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.
Artículo 23. Tiempo de la recepción de un mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:
Ley No. 43 de 2001 8
1. Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar en el momento en que ingrese el mensaje de datos en el sistema de información designado; o
2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos;
3. Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario.
Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al artículo siguiente.
Artículo 24. Lugar del envío y recepción del mensaje de datos. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:
1. Si el iniciador o el destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal;
2. Si el iniciador o el destinatario no tiene establecimiento, se tendrá en cuenta su lugar de residencia habitual.
Título II
Firmas y Certificados Electrónicos

CCaappíítuulloo IIII
FFiirrmmaass EElleeccttrróónniiccaass
Artículo 25. Atributos de la firma electrónica. El uso de una firma electrónica tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:
1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
Ley No. 43 de 2001 9
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma electrónica es inválida.
Artículo 26. Firma electrónica segura. Es una firma electrónica que puede ser verificada de conformidad con un sistema o procedimiento de seguridad, de acuerdo con estándares reconocidos internacionalmente.
Artículo 27. Mensaje de datos firmado electrónicamente. Se entenderá que un mensaje de datos ha sido firmado, si el símbolo o la metodología adoptada por la parte, cumple con un procedimiento de autenticación o seguridad.
CCaappíítuulloo IIII
CCeerrttiiffiiccaaddooss
Artículo 28. Contenido de los certificados. Un certificado emitido por una entidad de certificación, además de estar firmado electrónicamente por ésta, debe contener, por lo menos, lo siguiente:
1. Nombre, dirección y domicilio del suscriptor.
2. Identificación del suscriptor nombrado en el certificado.
3. Nombre, dirección y lugar donde realiza actividades la entidad de certificación.
4. Metodología para verificar la firma electrónica del suscriptor impuesta en el mensaje de datos.
5. Número de serie del certificado.
6. Fecha de emisión y expiración del certificado.
Artículo 29. Expiración de un certificado. Un certificado emitido por una entidad de certificación expira en la fecha indicada en él.
Artículo 30. Aceptación de un certificado. Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la entidad de certificación, a solicitud de éste o de una persona en nombre de éste, lo ha publicado en un repositorio o lo ha enviado a una o más personas.
Artículo 31. Garantía derivada de la aceptación de un certificado. El suscriptor, al momento de aceptar un certificado, garantiza a todas las personas de buena fe exentas de culpa, que se soportan en la misma información en él contenida, que:
1. La firma electrónica autenticada mediante éste, está bajo su control exclusivo;
Ley No. 43 de 2001 10
2. Ninguna persona ha tenido acceso al procedimiento de generación de la firma electrónica;
3. La información contenida en el certificado es verdadera y corresponde a la suministrada por éste a la entidad de certificación.
Artículo 32. Suspensión y revocación de certificados. El suscriptor de una firma certificada podrá solicitar a la entidad de certificación que expidió un certificado, la suspensión o renovación de éste. La revocación o suspensión del certificado se hace efectiva a partir del

momento en que se registra por parte de la entidad de certificación. Este registro debe hacerse en forma inmediata, una vez recibida la solicitud de suspensión o revocación.

Artículo 33. Causales para la revocación de certificados. El suscriptor de una firma electrónica certificada está obligado a solicitar la revocación del certificado en los siguientes casos:

1. Por pérdida de la información que da validez al certificado.
2. Si la privacidad del certificado ha sido expuesta o corre peligro de que se le dé un uso indebido.
3. Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por la pérdida o perjuicio en los cuales incurran terceros de buena fe exentos de culpa, que confiaron en el contenido del certificado.

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

a. Petición del suscriptor o un tercero en su nombre y representación.
b. Muerte del suscriptor.
c. Disolución del suscriptor, en el caso de las personas jurídicas.
d. Confirmación de que alguna información o hecho, contenido en el certificado, es falso.
e. La privacidad de su sistema de seguridad ha sido comprometida de manera material, que afecte la confiabilidad del certificado.
f. Cese de actividades de la entidad de certificación.
2. Orden judicial o de autoridad administrativa competente.

Ley No. 43 de 2001 11

Artículo 34. Notificación de la suspensión o revocación de un certificado. Una vez registrada la suspensión o revocación de un certificado, la entidad de certificación debe publicar, en forma inmediata, un aviso de suspensión o renovación en todos los repositorios en los cuales la entidad de certificación publicó el certificado. También deberá notificar de este hecho a las personas que soliciten información acerca de una firma electrónica verificable, por remisión al certificado suspendido o revocado.

Si los repositorios en los cuales se publicó el certificado no existen al momento de la publicación del aviso o son desconocidos, la entidad de certificación deberá publicar dicho aviso en un repositorio que designe la Dirección de Comercio Electrónico del Ministerio de Comercio e Industrias.

Artículo 35. Registro de certificados. Toda entidad de certificación deberá llevar un registro de los certificados emitidos, que se encuentre a disposición del público, el cual debe indicar las fechas de emisión, expiración y los registros de suspensión, revocación o reactivación de ellos.

Artículo 36. Término de conservación de los registros. Los registros de certificados expedidos por una entidad de certificación deben ser conservados por el término de quince años, contado a partir de la fecha de revocación o expiración del correspondiente.

CCaappíítuulloo IIIII

SSuuss cr iippttoorreess dee FFiirmmaass EElleecctrróónniiccaass

Artículo 37. Deberes de los suscriptores. Son deberes de los suscriptores:

1. Recibir los certificados por parte de la entidad de certificación, utilizando un sistema de seguridad exigido por la entidad de certificación con la que haya contratado sus servicios, o en un esquema de interoperabilidad para aceptar certificados reconocidos por diferentes entidades de certificación.
2. Suministrar información completa, precisa y verídica a la entidad de certificación con la que haya contratado sus servicios.

3. Aceptar los certificados emitidos por la entidad de certificación, demostrando aprobación de sus contenidos mediante el envío de éstos a una o más personas o solicitando la publicación de éstos en repositorios.
4. Mantener el control de la información que da privacidad al certificado y reservarla del conocimiento de terceras personas.
5. Efectuar oportunamente las correspondientes solicitudes de suspensión o revocación.
Ley No. 43 de 2001 12
Un suscriptor cesa en la obligación de cumplir con los anteriores deberes, a partir de la certificación de un aviso de revocación del correspondiente certificado por parte de la entidad de certificación.
Artículo 38. Solicitud de información. Los suscriptores podrán solicitar a la entidad de certificación información sobre todo asunto relacionado con los certificados y las firmas electrónicas.
Artículo 39. Responsabilidad de los suscriptores. Los suscriptores serán responsables por la falsedad o error en la información suministrada a la entidad de certificación y que es objeto material del contenido del certificado. También serán responsables en los casos en los cuales no den oportunamente el aviso de revocación o suspensión de certificados, en los casos indicados anteriormente.
Título III
Autoridad de Registro y Entidades de Certificación
Capítulo II
Autoridad de Registro Voluntario
Artículo 40. La Autoridad. Se crea dentro del Ministerio de Comercio e Industrias, la Dirección de Comercio Electrónico, adscrita a la Dirección Nacional de Comercio, como Autoridad de Registro Voluntario de Prestadores de Servicios de Certificación. La Dirección de Comercio Electrónico establecerá un sistema de acreditación mediante registro voluntario.
Por medio de la presente Ley, la Autoridad queda facultada para acreditar y supervisar a las entidades de certificación, de acuerdo con criterios establecidos en normas internacionales, a fin de garantizar un nivel básico de seguridad y calidad de sus servicios, que son de vital importancia para la confiabilidad de las firmas electrónicas. La expedición de certificados u otros servicios relacionados no estará sujeta a autorización previa.
Para realizar el registro voluntario, se deberá pagar una tasa por este servicio a la Autoridad, cuyo monto y procedimiento de pago será determinado por reglamento. Hasta que no haya sido dictado el reglamento, se establece que la tasa de registro será de mil balboas (B/.1,000.00).
Entre las funciones de la Autoridad se encuentran las siguientes:
1. Registrar a las entidades de certificación que así lo soliciten, conforme a la reglamentación expedida por el Ministerio de Comercio e Industrias.
Ley No. 43 de 2001 13
2. Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de toda entidad de certificación, y por el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad.
3. Dictar los reglamentos sobre la materia.
4. Revocar o suspender el registro de la entidad de certificación.
5. Requerir a las entidades de certificación que suministren información relacionada con los certificados, las firmas electrónicas emitidas y los documentos en soporte informático que custodien o administren, pero únicamente cuando se refieran a los procesos que afecten la

seguridad e integridad de datos. Esta función no permite el acceso al contenido de los mensajes, a las firmas o a los procesos utilizados, excepto mediante orden judicial.
6. Imponer sanciones a las entidades de certificación por el incumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio.
7. Ordenar la revocación o suspensión de certificados, cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales.
8. Designar los repositorios en los eventos previstos en la ley.
Las entidades de certificación que no lleven a cabo la acreditación voluntaria, quedarán sujetas a las facultades de inspección de la Autoridad de Registro, para los efectos de velar por el cumplimiento de las obligaciones correspondientes que establece esta Ley o sus reglamentos, así como al cumplimiento de las disposiciones legales sobre la materia.
Una vez presentada toda la documentación establecida para obtener la acreditación, la Autoridad de Registro dispondrá del término de noventa días para emitir criterio. De no efectuar ningún pronunciamiento al respecto, se entenderá que ha emitido criterio favorable y deberá procederse con el registro. Otorgada la acreditación, la entidad de certificación será inscrita en un registro que será de carácter público, que a tal efecto llevará la Autoridad y al cual se podrá tener acceso por medios electrónicos. La entidad de certificación tendrá la obligación de informar a la Autoridad de Registro cualquier modificación de las condiciones que permitieron su acreditación.
Artículo 41. La Contraloría General de la República como entidad certificadora. Para toda la documentación, firmas electrónicas, servicios de certificación, claves de descuentos y otros actos que afecten o puedan afectar fondos o bienes públicos, la entidad certificadora es la Contraloría General de la República.
Artículo 42. Infracciones y sanciones. Se consideran infracciones las siguientes:
Ley No. 43 de 2001 14
1. Incumplimiento de cualquiera de las disposiciones de esta Ley.
2. Negligencia en la prestación del servicio.
3. Comisión de delito en la prestación del servicio.
La Autoridad de Registro, de acuerdo con el debido proceso y el derecho de defensa, podrá imponer, según la naturaleza y la gravedad de la falta, las siguientes sanciones a las entidades de certificación que incumplan o violen las normas a las cuales debe sujetarse su actividad:
a. Amonestación.
b. Multa de cien balboas (B/.100.00) hasta cien mil balboas (B/.100,000.00).
c. Suspensión de inmediato de todas o algunas de las actividades de la entidad infractora.
d. Prohibición a la entidad de certificación infractora de prestar directa o indirectamente los servicios de la entidad de certificación por el término de hasta cinco años.
e. Revocación definitiva de la acreditación y prohibición para operar en Panamá como entidad de certificación, cuando la aplicación de las sanciones anteriormente enumeradas, no haya sido efectiva y se pretenda evitar perjuicios reales o potenciales a terceros.
Artículo 43. Recursos. Las resoluciones de la Autoridad de Registro podrán ser impugnadas por los interesados cuando consideren que han sido perjudicados en sus intereses legítimos o en sus derechos. Contra dichas resoluciones podrá ser interpuesto el Recurso de Reconsideración contra la propia Autoridad de Registro y/o de Apelación ante el Ministro de Comercio e Industrias. La Autoridad de Registro tendrá un plazo de dos meses para decidir el Recurso de Reconsideración interpuesto. Si en tal plazo no ha sido resuelto el Recurso, la decisión se considerará favorable al recurrente.

De la misma forma, el Ministro de Comercio e Industrias dispondrá de dos meses para resolver el Recurso de Apelación. Si en tal plazo no ha sido resuelto el Recurso, la decisión se considerará favorable al recurrente.

CAPÍTULO III

ENTIDADES DE CERTIFICACIÓN

Artículo 44. Naturaleza, características y requerimientos de las entidades de certificación. Podrá ser acreditada como entidad de certificación, toda persona nacional o extranjera, la cual podrá acreditarse de forma voluntaria en la Autoridad de Registro,

Ley No. 43 de 2001 15

cumpliendo con los requerimientos establecidos por la ley o sus reglamentos, con base en las siguientes condiciones:

1. Contar con la capacidad económica y financiera suficientes para prestar los servicios autorizados como entidad de certificación.
2. Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad.
3. Los representantes legales, administradores y personal operativo no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, o que hayan sido suspendidas en el ejercicio de su profesión por faltas graves contra la ética o hayan sido excluidas de aquélla.
4. Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos.
5. Emplear personal calificado para la presentación del servicio ofrecido.
6. Haber contratado un seguro apropiado.
7. Cumplir con el pago de las tasas que para tal efecto se establezcan mediante reglamento.

Artículo 45. Actividades de las entidades de certificación. Las entidades de certificación podrán realizar las siguientes actividades:

1. Emitir certificados en relación con las firmas electrónicas de personas naturales o jurídicas.
2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y la recepción del mensaje de datos.
3. Ofrecer o facilitar los servicios de creación de firmas electrónicas certificadas.
4. Ofrecer o facilitar los servicios de registro y estampado cronológico en la transmisión y recepción de mensajes de datos.
5. Ofrecer los servicios de archivo y conservación de mensaje de datos.
6. Cualquier otra actividad complementaria, conexa o afín con las aquí mencionadas.

Artículo 46. Evaluaciones técnicas a las entidades de certificación. Con el fin de comprobar el cumplimiento de las obligaciones de las entidades de certificación, la Autoridad de Registro ejercerá la facultad inspectora sobre éstas y podrá, a tal efecto, requerir información y ordenar evaluaciones técnicas de seguimiento o de renovación,

Ley No. 43 de 2001 16

por lo menos, una vez al año a sus instalaciones. Como resultado de las visitas de evaluación técnica, la Autoridad de Registro evaluará el desempeño de cada una de las entidades de certificación, formulando las recomendaciones y las medidas pertinentes que deben ser atendidas por las entidades de certificación para la prestación del servicio, de conformidad con las exigencias legales y reglamentarias.

Sin perjuicio de lo que dispone el presente artículo, la Autoridad de Registro podrá autorizar a otras entidades privadas o públicas, de conformidad con el reglamento respectivo, para llevar a cabo los análisis técnicos respectivos a la evaluación técnica.

Si como resultado de la evaluación se establece que la entidad de certificación no ha cumplido con los requerimientos legales y reglamentarios en el desempeño de sus

operaciones, la Autoridad podrá imponer cualquiera de las sanciones previstas en la presente Ley. El resultado de la evaluación será incluido en la manifestación de práctica de la correspondiente entidad de certificación. Esta manifestación de práctica deberá también publicarse en el repositorio que la Autoridad de Registro designe para tal efecto.

Artículo 47. Manifestación de práctica de la entidad de certificación. Cada entidad de certificación acreditada publicará, en un repositorio de la Autoridad de Registro o en el que ésta designe, una manifestación de práctica de entidad de certificación que contenga la siguiente información:

1. Nombre, dirección y número telefónico de la entidad de certificación.
2. Sistema electrónico de la entidad de certificación.
3. Resultado de la evaluación obtenida por la entidad de certificación en la última auditoría realizada por la Autoridad del Registro.
4. Si la acreditación para operar como entidad de certificación ha sido revocada o suspendida, o si con motivo de la auditoría se ha impuesto alguna sanción. Este registro deberá incluir igualmente la fecha de la revocación o suspensión y los motivos de ésta.
5. Límites para operar la entidad de certificación.
6. Cualquier evento que sustancialmente afecte la capacidad de la entidad de certificación para operar.
7. Lista de normas y procedimientos de certificación.
8. Denominación del sistema de seguridad y protección utilizado.
9. Método para la identificación de dicho sistema.

Ley No. 43 de 2001 17

10. Descripción del plan de contingencia que garantice los servicios.
11. Cualquier información que se requiera mediante reglamento.

Artículo 48. Remuneración por la prestación de servicios. La remuneración por los servicios de las entidades de certificación será establecida libremente por éstas.

Artículo 49. Deberes de las entidades de certificación. Las entidades de certificación tendrán, entre otros, los siguientes deberes:

1. Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.
2. Demostrar la fiabilidad necesaria de sus servicios.
3. 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.
4. Emplear personal calificado 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.
5. 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.
6. 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.
7. Emitir certificados conforme a lo solicitado o acordado por el suscriptor.
8. Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas electrónicas, la conservación y archivo de certificados y documentos en soporte de mensajes de datos.

9. Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
10. Garantizar la prestación permanente del servicio de la entidad de certificación.
11. Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores.
12. Efectuar los avisos y publicaciones, conforme a lo dispuesto en la presente Ley.
Ley No. 43 de 2001 18
13. Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos y, en general, sobre cualquier documento electrónico que se encuentre bajo su custodia y administración.
14. Actualizar permanentemente los medios tecnológicos, conforme a las especificaciones adoptadas mediante reglamento.
15. Permitir y facilitar la realización de las evaluaciones técnicas que ordene la Autoridad de Registro.
16. Publicar en un repositorio un listado de los certificados suspendidos o revocados.
17. Publicar en un repositorio su manifestación de práctica de entidad de certificación.
18. Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio.
19. Llevar un registro de los certificados.
Artículo 50. Terminación unilateral. Salvo acuerdo entre las partes, la entidad de certificación podrá dar por terminado el acuerdo de vinculación con el suscriptor, dando un preaviso no menor de noventa días. Vencido este término, la entidad de certificación revocará los certificados que se encuentren pendientes de expiración.
Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la entidad de certificación, dando un preaviso no inferior a treinta días.
Artículo 51. Responsabilidad de la entidad de certificación. Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que, en el ejercicio de su actividad, ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.
Sin perjuicio de lo dispuesto en el párrafo anterior, los prestadores de servicios de certificación no serán responsables de los daños o perjuicios que tengan en su origen el uso indebido o fraudulento de un certificado de firma electrónica por parte del suscriptor.
Los prestadores de servicios deberán disponer de los recursos económicos suficientes para operar, de conformidad con lo dispuesto en esta Ley, 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.
Ley No. 43 de 2001 19
Para los efectos de este artículo, los prestadores de servicios de certificación deberán acreditar la contratación y mantenimiento de una garantía que cubra su eventual responsabilidad civil contractual y extracontractual. El tipo, monto y procedimiento para consignar esta garantía será fijada mediante reglamento.
Artículo 52. Cesación de actividades por parte de las entidades de certificación. Las entidades de certificación podrán cesar en el ejercicio de actividades, siempre que hayan notificado a la Autoridad de Registro con cuatro meses de anticipación.
Una vez haya sido notificada la cesación de actividades, la entidad de certificación que cesará de operar, deberá enviar a cada suscriptor un aviso, con no menos de noventa días de anticipación a la fecha de la cesación efectiva de actividades, en el cual solicitará autorización

para revocar o publicar en otro repositorio de otra entidad de certificación, los certificados que aún se encuentran pendientes de expiración.
Pasados sesenta días sin obtenerse respuesta por parte del suscriptor, la entidad de certificación podrá revocar los certificados no expirados u ordenar su publicación, dentro de los quince días siguientes, en un repositorio de otra entidad de certificación, en ambos casos, dando aviso de ello al suscriptor.
Si la entidad de certificación no ha efectuado la publicación en los términos del párrafo anterior, la Autoridad ordenará la publicación de los certificados no expirados en los repositorios de la entidad de certificación por ella designada.
En el evento de no ser posible la publicación de estos certificados en los repositorios de cualquier entidad de certificación, la Autoridad efectuará la publicación de los certificados no expirados en un repositorio de su propiedad.

CAPÍTULO III
REPOSITORIOS

Artículo 53. Reconocimiento y actividades de los repositorios. La Autoridad de Registro autorizará únicamente la operación de los repositorios que mantengan las entidades de certificación acreditadas.
Los repositorios autorizados para operar deberán:
1. Mantener una base de datos de certificados, de conformidad con los reglamentos
2. respectivos.
Ley No. 43 de 2001 20
3. Garantizar que la información que mantienen se conserve íntegra, exacta y razonablemente confiable, de forma que pueda ser recuperada para su ulterior consulta.
4. Mantener un registro de las publicaciones de los certificados revocados o suspendidos.

CAPÍTULO IV
DISPOSICIONES VARIAS

Artículo 54. Certificaciones recíprocas. Los certificados emitidos por entidades de certificación extranjeras podrán ser reconocidos en los mismos términos y condiciones exigidos en ella para la emisión de certificados por parte de las entidades de certificación nacionales, cuando:
1. Tales certificados sean reconocidos por una entidad de certificación acreditada en Panamá que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.
2. Tales certificados sean reconocidos en virtud de acuerdos con otros países, ya sean bilaterales o multilaterales, o efectuados en el marco de organizaciones internacionales de las que Panamá sea parte.
3. Tales certificados sean aceptados en virtud de su validez, de acuerdo con estándares internacionalmente reconocidos y éstos sean emitidos por entidades de certificación, debidamente avalados en su país de origen, por autoridades homólogas a la Autoridad de Registro panameña.
Artículo 55. Incorporación por remisión. Salvo acuerdo en contrario entre las partes, cuando en un mensaje de datos se haga remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente, se presume que estos términos están incorporados por remisión a ese mensaje de datos. Entre las partes, y conforme a la ley, estos términos serán jurídicamente válidos como si hubieran sido incorporados en su totalidad en el mensaje de datos.

Ley No. 43 de 2001 21
Título IV
Reglamentación y Vigencia
CCaappíítuulloo II
DDiissppoossiicciioonneess VVaarriiaass
Artículo 56. Las entidades de certificación que hayan iniciado la prestación de sus servicios con anterioridad a la entrada en vigencia de la presente Ley, deberán adecuar sus actividades a lo dispuesto en ella dentro de los seis meses contados a partir de la promulgación del reglamento respectivo.
Artículo 57. El Órgano Ejecutivo deberá reglamentar la presente Ley dentro de los seis meses siguientes a su entrada en vigencia, en lo que se refiere al funcionamiento de la Autoridad de Registro y demás aspectos contenidos dentro de la presente Ley. El Órgano Ejecutivo realizará consultas con el sector privado para la promulgación de leyes y reglamentos sobre esta materia, así como para hacer recomendaciones y actualizaciones periódicas, con el fin de contemplar innovaciones por avances tecnológicos.
CCaappíítuulloo IIII
VVii gg eenn cc iiaa
Artículo 58. Vigencia y derogatoria. La presente Ley entrará a regir desde su promulgación y deroga las normas que le sean contrarias.
COMUNÍQUESE Y CÚMPLASE.
Aprobada en tercer debate, en el Palacio Justo Arosemena, ciudad de Panamá, a los días del mes de junio del año dos mil uno.
El Presidente,
Laurentino Cortizo Cohen
El Secretario General Encargado,
Jorge Ricardo Fábrega
Ley No. 43 de 2001 22

ANEXO 6

LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO.

LEY MODELO
DE LA CNUDMI
SOBRE COMERCIO ELECTRÓNICO

1996

con la adición del Artículo 5 bis en la forma aprobada en 1998

NACIONES UNIDAS

ÍNDICE

Resolución aprobada por la Asamblea General

[sobre la base del informe de la Sexta Comisión (A/51/628)]

51/162. *Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*

La Asamblea General,

Recordando su resolución 2205 (XXI), de 17 de diciembre de 1966, por la que estableció la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional con el mandato de fomentar la armonización y la unificación progresivas del derecho mercantil internacional y de tener presente, a ese

respecto, el interés de todos los pueblos, en particular el de los países en desarrollo, en el progreso amplio del comercio internacional,

Observando que un número creciente de transacciones comerciales internacionales se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, habitualmente conocidos como "comercio electrónico", en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel,

Recordando la recomendación relativa al valor jurídico de los registros computadorizados aprobada por la Comisión en su 18. período de sesiones, celebrado en 1985, y el inciso *b)* del párrafo 5 de la resolución 40/71 de la Asamblea General, de 11 de diciembre de 1985, en la que la Asamblea pidió a los gobiernos y a las organizaciones internacionales que, cuando así convenga, adopten medidas acordes con las recomendaciones de la Comisión a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos en el comercio internacional,

Convencida de que la elaboración de una ley modelo que facilite el uso del comercio electrónico y sea aceptable para Estados que tengan sistemas jurídicos, sociales y económicos diferentes podría contribuir de manera significativa al establecimiento de relaciones económicas internacionales armoniosas,

Observando que la Ley Modelo sobre Comercio Electrónico fue aprobada por la Comisión en su 29. período de sesiones después de examinar las observaciones de los gobiernos y de las organizaciones interesadas,

Estimando que la aprobación de la Ley Modelo sobre Comercio Electrónico por la Comisión ayudará de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación en los casos en que carezcan de ella,

1. *Expresa su agradecimiento* a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional por haber terminado y aprobado la Ley Modelo sobre Comercio Electrónico que figura como anexo de la presente resolución y por haber preparado la Guía para la Promulgación de la Ley Modelo;

2. *Recomienda* que todos los Estados consideren de manera favorable la Ley Modelo cuando promulguen o revisen sus leyes, habida cuenta de la necesidad de que el derecho aplicable a los métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel sea uniforme;

3. *Recomienda también* que no se escatimen esfuerzos para velar por que la Ley Modelo y la Guía sean ampliamente conocidas y estén a disposición de todos.

85a. sesión plenaria
16 de diciembre de 1996

LEY MODELO DE LA CNUDMI SOBRE COMERCIO ELECTRÓNICO

[Original: árabe, chino, español, francés, inglés, ruso]

PRIMERA PARTE

Comercio electrónico en general

Capítulo I

Disposiciones generales

Artículo 1

*Ámbito de aplicación**

La presente Ley** será aplicable a todo tipo de información en forma de mensaje de datos utilizada en el contexto*** de actividades comerciales****.

---

* La Comisión sugiere el siguiente texto para los Estados que deseen limitar el ámbito de aplicación de la presente Ley a los mensajes de datos internacionales:

- La presente Ley será aplicable a todo mensaje de datos que sea conforme a la definición del párrafo 1) del artículo 2 y que se refiera al comercio internacional.

** La presente ley no deroga ninguna norma jurídica destinada a la protección del consumidor.

*** La Comisión sugiere el siguiente texto para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley:

La presente Ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en las situaciones siguientes: [...].

**** El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Artículo 2

Definiciones

Para los fines de la presente Ley:

a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a 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;

d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él;

e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Artículo 3

Interpretación

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

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

Artículo 4

Modificación mediante acuerdo

1) Salvo que se disponga otra cosa, en las relaciones entre las partes que generan envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del capítulo III podrán ser modificadas mediante acuerdo.

2) Lo dispuesto en el párrafo 1) no afectará a ningún derecho de que gocen las partes para modificar de común acuerdo alguna norma jurídica a la que se haga referencia en el capítulo II.

Capítulo II

Aplicación de los requisitos jurídicos a los mensajes de datos

Artículo 5

Reconocimiento jurídico de los mensajes de datos

No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

Artículo 5 bis

Incorporación por remisión

(En la forma aprobada por la Comisión en su 31.º período de sesiones, en junio de 1998)

No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.

Artículo 6

Escrito

1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7

Firma

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 8

Original

1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

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

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

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del inciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

4) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 9

Admisibilidad y fuerza probatoria de los mensajes de datos

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

a) Por la sola razón de que se trate de un mensaje de datos; o

b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Artículo 10

Conservación de los mensajes de datos

1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su ulterior consulta; y

b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y

c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.

2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1).

Capítulo III

Comunicación de los mensajes de datos

Artículo 11

Formación y validez de los contratos

1) En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 12

Reconocimiento por las partes de los mensajes de datos

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

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 13

Atribución de los mensajes de datos

1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.

2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:

a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o

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

3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de datos proviene del iniciador, y a actuar en consecuencia, cuando:

a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o

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

4) El párrafo 3) no se aplicará:

a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o

b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.

5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.

6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.

Artículo 14

Acuse de recibo

1) Los párrafos 2) a 4) del presente artículo serán aplicables cuando, al enviar o antes de enviar un mensaje de datos, el iniciador solicite o acuerde con el destinatario que se acuse recibo del mensaje de datos.

2) Cuando el iniciador no haya acordado con el destinatario que el acuse de recibo se dé en alguna forma determinada o utilizando un método determinado, se podrá acusar recibo mediante:

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

b) Todo acto del destinatario,

que basten para indicar al iniciador que se ha recibido el mensaje de datos.

3) Cuando el iniciador haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo.

4) Cuando el iniciador no haya indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, si no ha recibido acuse en el plazo fijado o convenido o no se ha fijado o convenido ningún plazo, en un plazo razonable el iniciador:

a) Podrá dar aviso al destinatario de que no ha recibido acuse de recibo y fijar un plazo razonable para su recepción; y

b) De no recibirse acuse dentro del plazo fijado conforme al inciso a), podrá, dando aviso de ello al destinatario, considerar que el mensaje de datos no ha sido enviado o ejercer cualquier otro derecho que pueda tener.

5) Cuando el iniciador reciba acuse de recibo del destinatario, se presumirá que éste ha recibido el mensaje de datos correspondiente. Esa presunción no implicará que el mensaje de datos corresponda al mensaje recibido.

6) Cuando en el acuse de recibo se indique que el mensaje de datos recibido cumple con los requisitos técnicos convenidos o enunciados en alguna norma técnica aplicable, se presumirá que ello es así.

7) Salvo en lo que se refiere al envío o recepción del mensaje de datos, el presente artículo no obedece al propósito de regir las consecuencias

jurídicas que puedan derivarse de ese mensaje de datos o de su acuse de recibo.

Artículo 15

Tiempo y lugar del envío y la recepción de un mensaje de datos

1) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando entre en un sistema de información que no esté bajo el control del iniciador o de la persona que envió el mensaje de datos en nombre del iniciador.

2) De no convenir otra cosa el iniciador y el destinatario, el momento de recepción de un mensaje de datos se determinará como sigue:

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

i) En el momento en que entre el mensaje de datos en el sistema de información designado; o

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

b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar al entrar el mensaje de datos en un sistema de información del destinatario.

3) El párrafo 2) será aplicable aun cuando el sistema de información esté ubicado en un lugar distinto de donde se tenga por recibido el mensaje conforme al párrafo 4).

4) De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente párrafo:

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

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

5) Lo dispuesto en el presente artículo no será aplicable a: [...].

SEGUNDA PARTE

Comercio electrónico en materias específicas

Capítulo I

Transporte de mercancías

Artículo 16

Actos relacionados con los contratos de transporte de mercancías

Sin perjuicio de lo dispuesto en la parte I de la presente Ley, el presente capítulo será aplicable a cualquiera de los siguientes actos que guarde relación con un contrato de transporte de mercancías, o con su cumplimiento, sin que la lista sea exhaustiva:

a)

i) indicación de las marcas, el número, la cantidad o el peso de las mercancías;

ii) declaración de la índole o el valor de las mercancías;

iii) emisión de un recibo por las mercancías;

iv) confirmación de haberse completado la carga de las mercancías;

b)

i) notificación a alguna persona de las cláusulas y condiciones del contrato;

ii) comunicación de instrucciones al portador;

c)

i) reclamación de la entrega de las mercancías;

ii) autorización para proceder a la entrega de las mercancías;

iii) notificación de la pérdida de las mercancías o de los daños que hayan sufrido;

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

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

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

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

Artículo 17

Documentos de transporte

1) Con sujeción a lo dispuesto en el párrafo 3), en los casos en que la ley requiera que alguno de los actos enunciados en el artículo 16 se lleve a cabo por escrito o mediante un documento que conste de papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no se lleve a cabo el acto por escrito o mediante un documento.

3) Cuando se conceda algún derecho a una persona determinada y a ninguna otra, o ésta adquiera alguna obligación, y la ley requiera que, para que ese acto surta efecto, el derecho o la obligación hayan de transferirse a esa persona mediante el envío, o la utilización, de un documento, ese

requisito quedará satisfecho si el derecho o la obligación se transfiere mediante la utilización de uno o más mensajes de datos, siempre que se emplee un método fiable para garantizar la singularidad de ese mensaje o esos mensajes de datos.

4) Para los fines del párrafo 3), el nivel de fiabilidad requerido será determinado a la luz de los fines para los que se transfirió el derecho o la obligación y de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

5) Cuando se utilicen uno o más mensajes de datos para llevar a cabo alguno de los actos enunciados en los incisos f) y g) del artículo 16, no será válido ningún documento utilizado para llevar a cabo cualquiera de esos actos, a menos que se haya puesto fin al uso de mensajes de datos para sustituirlo por el de documentos. Todo documento que se emita en esas circunstancias deberá contener una declaración a tal efecto. La sustitución de mensajes de datos por documentos no afectará a los derechos ni a las obligaciones de las partes.

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

7) Lo dispuesto en el presente artículo no será aplicable a: [...].