UNIVERSIDAD CENTROAMERICANA

TRABAJO MONOGRÁFICO PARA OBTENER EL TÍTULO DE LICENCIADO EN DERECHO

"LA SEGURIDAD JURÍDICA EN LA CONTRATACIÓN ELECTRÓNICA"

Autores

Indira Jahosca Blandón Lagos

Gema Auxiliadora Campos Ayala

Tutor

Msc. Cristian Robleto Arana

Septiembre, 2010

DEDICATORIA

A Dios por ser nuestra guía y darnos la oportunidad de ser cada día alguien mejor y por darnos entendimiento y sabiduría para discernir todos los conocimientos obtenidos; a nuestros padres por habernos apoyado a lo largo de nuestra carrera, por llenarnos con palabras de aliento, por hacer suyos nuestros desvelos y preocupaciones y por contribuir con nuestra perfección; a nuestros profesores por ser un ejemplo, por armarse de paciencia y por depositar sus esperanzas en nosotras, esa esperanza de vernos llegar alto; y a todas aquellas personas que han estado a nuestro lado apoyándonos incondicionalmente.

CONTENIDO

OBJETIVOS

Objetivo general

1. Desarrollar las instituciones que dan seguridad jurídica a la contratación electrónica.

Objetivos Específicos

1- Explicar cómo la sociedad de información ha dado lugar a la creación de nuevas figuras tecnológicas.

2- Establecer el concepto de un contrato electrónico, la forma en que éste nace y su perfeccionamiento.

3- Desarrollar el concepto de la firma electrónica según la doctrina y legislaciones de diferentes países.

4- Estudiar las entidades de certificación como elemento de seguridad jurídica en el comercio electrónico.

5- Recalcar la afectación que producen los delitos cometidos por medio de la red.

DISEÑO METODOLÓGICO

Para llevar a cabo esta investigación se utilizará el método analítico crítico, ya que éste nos permitirá tanto el análisis de los aspectos relativos a la Seguridad Jurídica que proporcionan las contrataciones electrónicas en el comercio electrónico, como el análisis de algunas leyes a nivel nacional e internacional que se encargan de regular las relaciones comerciales. De manera breve se hará una crítica acerca de la falta de regulación jurídica existente en nuestro país.

CAPITULO I.

LA SOCIEDAD DE INFORMACION, GENERALIDADES

1. INTRODUCCIÓN

En el mundo actual día a día se trata de construir una sociedad que permita acceder de manera igualitaria a la enorme cantidad de información que circula por los medios.

Hoy por hoy la llamada “Sociedad de la Información” está dando origen a un sin número de cambios en nuestra sociedad. Esto se debe a los incontables medios que día a día surgen y que permiten la circulación de información, principalmente mediante la vía digital.

El crecimiento de las tecnologías en general, y de las tecnologías de la información en particular, han servido para facilitar la vida de nuestra sociedad en todos los sentidos. Así se observa que las relaciones entre las personas son cada día más frecuentes y cercanas gracias a los medios electrónicos, los que han posibilitado novedosas formas de interrelacionarnos con los demás no importando si podemos o no ver a esa persona: con un solo click nos comunicamos, entretenemos y hasta compramos o vendemos a través de la red.

Es de suma importancia atender a la forma en que se están regulando las relaciones comerciales, ya que el uso de la red, además de traer beneficios, puede dar lugar a la comisión de un sin número de ilícitos.

En el presente trabajo se tratará de aclarar lo que es la Sociedad de Información, espacio del que surgen una serie de nuevas ideas en continuo crecimiento y que necesitan aclaración.

Para lograr el tremendo desarrollo tecnológico de la actual sociedad de la comunicación global e instantánea, ésta ha tenido que pasar por numerosas etapas desde tiempos remotos, en donde a lo único que se tenía acceso era a un sistema de correos lento y poco seguro. En el siglo XX empezaron a desarrollarse medios de mayor progreso e inmediatez, ahora ya vistos como un tanto convencionales, tales como el telégrafo, la radio, el teléfono y la televisión.

Con los cambios a los que dio lugar esta sociedad globalizada y posmoderna de hoy, se han producido nuevas ideas y manifestaciones tecnológicas surgidas en el seno de dicha Sociedad de la Información. Ejemplos claros de esto es lo que hoy conocemos como comercio electrónico y gobierno electrónico, de los que se dará una aclaración para ofrecer una idea de las gigantescas bases de información a las que se puede tener acceso hoy en día.

Además, se profundizará en los contratos electrónicos y la seguridad jurídica que éstos proporcionan a todo aquel que realice sus actividades comerciales por medio de la red. También se incluirán en el desarrollo de este trabajo el análisis de las entidades de certificación y de la firma electrónica: la identificación de la misma entidad de certificación y la constatación de la veracidad y de la legitimidad de las firmas electrónicas o la integridad de un mensaje.

Un gran número de países han puesto en marcha sus normas para tratar de hacer frente a las nuevas concepciones adoptadas en la sociedad, como las mencionadas anteriormente.

Actualmente en nuestro país se habla mucho de la llamada firma electrónica, sobre la que ya se realizó un anteproyecto, el cual viene a regularla y que aún está en el seno de la Asamblea Nacional, esperando ser aprobado.

En el presente trabajo investigativo se planteará también lo relacionado con los delitos informáticos, lo cual ha cobrado vida mediante la red de redes, la internet.

2. ANTECEDENTES

Debido a los procesos de transformación que ha sufrido la sociedad de información, se tomará como punto de referencia a la sociedad industrial, ya que se dice que la Sociedad de Información es vista como la sucesora de la sociedad industrial.

La sociedad industrial es el conjunto de actividades económicas que tiene por objeto la transformación masiva de materias primas a productos elaborados, los que pueden satisfacer directamente las necesidades de la población, por medio de un proceso mecánico, con división y especialización del trabajo, lo que permite aumentar la producción.

Anónimo (2008), relata que hoy en día la sociedad ha sido transformada por una nueva e importante revolución científica y tecnológica que comienza a desarrollarse en la década de los 60. Ya para esta fecha se empieza a hablar de la sociedad post-industrial o sociedad de la información, como mejor se la conoce, donde más que usar la fuerza física del hombre lo que se utiliza es el esfuerzo intelectual, es decir que esta nueva sociedad cambió la visión de las cosas, debido a que ya no se toma a las máquinas como instrumento fundamental para la economía, sino que se ve más allá de lo que el hombre puede lograr por medio de las creaciones de su intelecto.

Refiere Contreras Díaz, Y, L y Rivero Amador, S, (2007) que en la década de los 70 cuando ya ha sido introducida la noción de lo que es la sociedad de información, surge el eslogan “La información es poder”. Esto da chance a una serie de cambios que configuran nuevas pautas sociales las cuales fueron motivadas por el sector servicio, esto debido a que ya no se tratará de desarrollar bienes tangibles, como estaba sucediendo en la sociedad industrial, sino que se pretende producir bienes que se ligan principalmente a la obtención de información.

Esta expresión reaparece con fuerza en los años 90, en el contexto del desarrollo de la Internet y de las Tecnologías de Información y Comunicación (TIC). Según

Téllez, J (2003 p.p 8), “las TIC son capitales para la creación de la sociedad mundial de la información y desempeñan un papel importante en la lucha contra la pobreza y la desigualdad a escala mundial”.

Según Rodríguez, (Agosto, 2005) a partir de 1995, la sociedad de información fue incluida en la agenda de las reuniones del grupo de los principales siete países industriales (G7), el cual es descrito por el Fondo Monetario Internacional (Marzo, 2010), como un foro para el análisis de los problemas económicos y financieros entre los países industriales más importantes del mundo. Posteriormente también se abordó el tema de la sociedad de información en el grupo G8, que pasó a llamarse así debido a la inclusión de Rusia. Esto se realizó con el fin de introducir el G8 su propia versión de la sociedad global de la información, ofreciendo una vez más, unas cuantas concentraciones para promover el servicio universal.

Asimismo señala Burch, (2010), que dada la importancia del tema de la Sociedad de Información éste se ha abordado en foros de la Comunidad Europea y de la OCDE (los treinta países más desarrollados del mundo), y también ha sido asumido por el gobierno de los Estados Unidos, así como por varias agencias de las Naciones Unidas y por el Banco Mundial.

A partir de 1998, la Sociedad de Información fue elegida, primero en la Unión Internacional de Telecomunicaciones y luego en la ONU, como tema central para la Cumbre Mundial a realizarse en 2003 y 2005, con el nombre de “La cumbre mundial sobre la Sociedad de la Información, Ginebra 2,003- Túnez 2,005”. Burch, (2010).

En base a la bibliografía consultada puede decirse que el objetivo de la Sociedad de Información, es lograr que los países subdesarrollados rompan esa brecha que les impide acceder a todo el conocimiento existente y se conviertan en países capaces de producir información a su población. Esto se logra según Burch, S, (2010) con la ayuda y la colaboración de organismos multilaterales como la Organización Mundial del Comercio (OMC), el Fondo Monetario Internacional (FMI) y el Banco Mundial.

Desde una perspectiva legal Castillo Jiménez, (2010), plantea que en 1968, por primera vez Naciones Unidas dicta una resolución en torno a los peligros que pueden derivarse del uso de las nuevas tecnologías y la protección de los derechos fundamentales, como el honor y la intimidad.

En cuanto a esto, señala García Pérez, J. F. (2010) que "Gran Bretaña fue el primer país en considerar las problemáticas presentadas en los formatos electrónicos".

Anónimo (2006), plantea que "la regulación de todo lo relacionado con Internet se ha dado a través de algunos decretos ejecutivos y directrices de la administración".

En 1997 se dictó una norma que declara de interés público el acceso a Internet (Decreto Ejecutivo Nº 26628-MICIT) y establece que este acceso debe darse en condiciones sociales y geográficas equitativas, con tarifas razonables y con Parámetros de calidad acordes a las modernas aplicaciones tecnológicas.

Respecto a la regulación de materias relacionadas con la firma electrónica, **Colombia** fue el primer país en instaurar una norma que regula todo el compendio de relaciones creadas por medios electrónicos con su ley 527 del 18 de agosto de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico, las firmas digitales, y se establecen las entidades de certificación.

En el **Perú** el 28 de mayo de 2000, se expidió la Ley de Firmas y Certificados Digitales No 27269 y posteriormente, el Decreto Supremo No 004-2007-PCM, por el cual se aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.

En Junio del 2001 se aprueba en **Panamá** la Ley No. 43; ley que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico y en el intercambio de documentos electrónicos.

En el 2002 nace en **España** la *Ley 34, del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, la cual en su Arto. 1 establece: **"**Es

objeto de la presente Ley 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 la información."

El 25 de marzo de este mismo año en **Chile** se expidió la ley 19799, sobre documentos electrónicos, firma electrónica y los servicios de certificación. Consecutivamente mediante el Decreto Nº 181 de fecha 9 de julio de 2002 se aprobó el reglamento de esta ley.

Para Junio en el año 2004 en **Puerto Rico** se aprueba la Ley No. 151, *Ley de Gobierno Electrónico,* la cual en su exposición de motivos plantea que la aplicación por el gobierno de las tecnologías de la información le brinda la oportunidad de mejorar la prestación de servicios al ciudadano, el desempeño de las funciones gubernamentales y la divulgación de información gubernamental, contribuyendo así a facilitar la participación de los ciudadanos en el gobierno.

En el 2005 se ejecutó la Ley de certificados, firmas digitales y documentos electrónicos en **Costa Rica** y entró a regir en el país el reglamento de la firma digital el 21 de Abril del 2006.

Así también **Argentina,** se vio la necesidad de crear normas para proteger datos, por lo que el 14 de noviembre de 2001, se sancionó la Ley No 25.506 sobre firma digital, en la cual se regularon aspectos como los certificados digitales.

Guatemala es uno más de los países que ha logrado formar parte de los estados que cuentan con regulaciones sobre actos que son realizados mediante modelos electrónicos. En el 2008 se publicó el decreto 47/2008, Ley para el reconocimiento de las comunicaciones y firmas electrónicas.

En la actualidad Nicaragua está avanzando poco a poco en cuanto al marco regulatorio de la llamada Sociedad de Información. Pese a este lento avance hemos encontrado tanto leyes como anteproyectos que hacen referencia a dichas sociedades.

De esta manera encontramos el Anteproyecto de Ley de Comercio Electrónico de nuestro país del 2007.

La reforma a las Normas Financieras del Banco Central de Nicaragua, Resolución CD-BCN-14-3-09, forma un precedente de la Sociedad de la Información, y plantea en el Arto.1:" El presente reglamento tiene por objeto regular la captación de recursos por parte del Banco Central de Nicaragua (en adelante denominado:"el BCN"), mediante la colocación de valores desmaterializados y estandarizados (letras y bonos) bajo las modalidades de subastas competitivas y no competitivas que efectuará el BCN a través del sistema de subasta electrónica que este ha desarrollado, las cuales les permite a los inversionistas previamente registrados en el BCN, ingresar sus ofertas de adquisición de valores estandarizados. (Reforma a las Normas Financieras del Banco Central de Nicaragua, Resolución CD-BCN-14-3-09.)

En la misma reforma se menciona la anotación en cuenta electrónica y plantea en el Arto.3 inciso A: se refiere al asiento contable efectuado en el registro contable de valores. (Reforma a las Normas Financieras del Banco Central de Nicaragua, Resolución CD-BCN-14-3-09).

En Octubre del 2006 en Nicaragua fue aprobada la ley No. 587, "Ley de Mercado de Capitales", la cual en su Arto. 1° menciona su objeto, el cual es regular los mercados de valores, las personas naturales y jurídicas que intervengan directa o indirectamente en ello, los actos o contratos relacionados con tales mercados y los valores negociados en ellos, debiendo promover las condiciones de transparencia y competitividad que hagan posible el buen funcionamiento del mercado, mediante la

difusión de cuanta información resulte necesaria para este fin, procurando la protección de los inversionistas.

La Bolsa de Valores de Nicaragua**,** (2010) establece que todas las transacciones realizadas en el seno de la Bolsa de Valores de Nicaragua (BVDN) se realizan a través de un sistema de negociación electrónico en el cual todos los Puestos de Bolsa están conectados a una red informática que administra la BVDN a través de un software desarrollado por esta; los puestos de bolsa venden y compran valores en el mercado primario, secundario, opciones y reportos. Asimismo los Puestos de Bolsa tienen acceso a toda la información histórica contendida en nuestras bases de datos.

Es por esto que la ley No. 587, "Ley de Mercado de Capitales" tiene gran relevancia ya que viene a regular un sistema de negociación vía electrónica, lo cual por el hecho de manifestarse por medio de la red forma parte de la sociedad de información.

3. Algunas manifestaciones de la Sociedad de Información.

Antes que nada es importante mencionar lo que se entiende por sociedad de la informacion; respecto a esto plantea Gil, J. M. (2004) que La comisión Europea en 1997 definió a la Sociedad de Información como aquella Sociedad en la que se utilizan tecnologías de transmisión y almacenamiento de información y datos de bajo costo.

3.1 Comercio Electrónico

Plantean Campiteni, A y Rosso, C, L (2010) que el Comercio Electrónico es una metodología moderna para hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como la mejora de la calidad de los bienes y servicios y el tiempo de entrega de éstos. Por lo tanto no debe seguirse contemplando el comercio electrónico como una tecnología, sino

que es el uso de la tecnología para mejorar la forma de llevar a cabo las actividades empresariales.

3.2 Firma digital y Firma electrónica.

Refiere Anónimo (2010) que los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto.

Mientras que la firma digital hace referencia a una serie de métodos criptográficos, la firma electrónica es un término de naturaleza fundamentalmente legal y más amplio desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

3.3 Gobierno Electrónico

Se establece según Anónimo (2010) “Que el e-government, e-gobierno o gobierno electrónico consiste en el uso de las tecnologías de la información y el conocimiento en los procesos internos de gobierno y en la entrega de los productos y servicios del Estado tanto a los ciudadanos como a la industria. Muchas de las tecnologías involucradas y sus implementaciones son las mismas o similares a aquéllas correspondientes al sector privado del comercio electrónico (o *e-business*), mientras que otras son específicas o únicas en relación a las necesidades del gobierno”.

CAPITULO II.

SEGURIDAD JURÍDICA DE LOS CONTRATOS CELEBRADOS POR VÍA ELECTRÓNICA

Para determinar cuál es la seguridad jurídica de los contratos celebrados a través de medios no convencionales como lo son los medios electrónicos, hay que precisar qué es el comercio electrónico y la forma en que dichos contratos se clasifican según la doctrina.

1. Comercio electrónico

Anónimo (2010) define al comercio electrónico como cualquier actividad que involucre a empresas que interactúan y hacen negocios por medios electrónicos, con clientes, otras empresas, o con el gobierno, incluyendo el pedido y el pago electrónico de bienes y servicios.

En lo referente a la legislación colombiana, ésta expresa en su ley 527 de 1999 que el comercio electrónico abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, y estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.

Por su parte las leyes 18.600 de Uruguay, “Documento electrónico y firma electrónica” y la ley 8454 de Costa Rica, “Ley de certificados, firmas digitales y documentos electrónicos”, no contemplan un concepto de lo que es el comercio electrónico, y es que éstas son más específicas en cuanto a lo que es la firma electrónica. En contraste mientras la legislación colombiana en relación a esta materia tiene un contenido más extenso al incluir el comercio electrónico, cuestión que ha llevado presente capítulo.

1.1 A continuación hacemos una breve **clasificación del comercio electrónico** con base en la doctrina. En relación a esto plantea Anónimo (2010) la siguiente clasificación:

1.1.1 Según bienes o servicios que se comercializan:

1.1.2 Comercio electrónico indirecto: consiste en adquirir bienes tangibles que necesitan luego ser enviados físicamente usando canales tradicionales de distribución. Ejemplo: libros, mercancía, etc.

1.1.3 Comercio electrónico directo: en este caso, el pedido, el pago y el envío de los bienes son intangibles, o sea, se producen vía on-line. Ejemplo: software, música, etc.

1.2 Según las partes que hacen la transacción:

1.2.1 Empresa-Empresa: una empresa realiza pedidos de materia prima a sus proveedores por Internet.

1.2.2 Empresa-Consumidor: se refiere a una empresa que vende sus productos o servicios a través de Internet. Ejemplo: vestimenta, discos.

1.2.3 Gobierno-Ciudadano: más que negocios propiamente dicho se refiere a trámites o impuestos por Internet.

1.2.4 Gobierno-Empresa: en los países como Estados Unidos, las transacciones y disposiciones entre éstos se hacen vía Internet.

1.2.5 Consumidor-Consumidor: esto se conoce como subastas por Internet, donde el consumidor ofrece a otro, sin mediar con una empresa, bienes y servicios.

Para que el comercio electrónico proporcione mayor seguridad jurídica a los empresarios o cualquier persona que desee mantener sus relaciones comerciales

mediante la red es necesario disponer de un servicio que emita certificados, lo cual se desarrollará más adelante.

2. Contratos electrónicos.

Antes que nada habría que señalar lo que se entiende por contrato y según lo que se ha estudiado no es más que un acuerdo de voluntades que genera obligaciones entre las partes, por lo que establece el Arto. 2435 del código civil de Nicaragua que "Contrato es un acuerdo de dos o más personas para constituir, regular o aclarar entre las mismas un vínculo jurídico".

Ya que se ha definido con la ayuda del código civil de Nicaragua el significado de un contrato como tal, cabe mencionar que debido al vertiginoso desarrollo de nuevas tecnologías, han surgido también nuevas estrategias de comercialización en los contratos electrónicos.

Este tipo de contratos es siempre un acuerdo de voluntad al igual que un contrato como tal. Así se ha establecido según el código civil de nuestro país; la diferencia radica en que los contratos electrónicos se realizan mediante la red y sin la utilización del papel.

Márquez, J, F, (2002) afirma que Las "Uniform Rules and Guidelines for Electronic Trade and Settlement (URGETS)", de la Cámara de Comercio Internacional (ICC), aplicables a contratos electrónicos en los cuales las partes se sometan a sus disposiciones, en su art. 3.1 define al contrato electrónico como *"el acuerdo con fuerza legal concluido a través del intercambio de mensajes electrónicos, concernientes a una o más transacciones comerciales electrónicas, en el cual las partes acuerdan los términos y condiciones del convenio, incluyendo sus derechos y obligaciones"*.

3. Formación del contrato electrónico.

Cabe mencionar que tanto en la contratación electrónica como en la contratación tradicional deben de realizarse un sin número de procedimientos a seguir para

llegar a obtener una relación comercial exitosa, es por esto que nos parece conveniente ocuparnos de dichos procedimientos.

3.1 Negociación

Señala Nieto Melgarejo, P (2010) que en la negociación las personas ejercen su libertad de contratar. Pueden negociar, pero aún no contratar. La negociación no obliga, es una esfera de libertad: no hay contrato en ese momento ni lo tiene que haber necesariamente, es sólo una posibilidad. Pero no sólo hay una frontera jurídica que limita la autonomía privada sino también una frontera moral, es decir se debe negociar sometiéndose al principio de buena fe. Se debe negociar con lealtad, y una forma de mantener la buena fe y la lealtad al momento de la contratación, es dotar de la información necesaria al consumidor para que este pueda decidir si contrata o no.

3.2 Publicidad

Antes que nada se definirá lo que se entiende por publicidad. Según el Arto. 2° de la Ley General de Publicidad Española, "publicidad es toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, industrial, artesanal o profesional, con el fin de promover de forma directa la contratación de bienes muebles o inmuebles, servicios, derechos y obligaciones".

Indica Nieto Melgarejo, P (2010) en relación a la publicidad, que la contratación electrónica se inicia normalmente mediante una comunicación comercial de un empresario profesional (el prestador de servicios de la sociedad de la información). Dicha comunicación comercial puede enviarse específicamente a una persona determinada o a varios destinatarios a través de correo electrónico o cualquier otro medio similar o, lo que es más frecuente, es puesta a disposición del público a través de un sitio Web.

En relación a la información que se difunde por Internet, ésta tendrá la consideración de publicidad en sentido legal cuando dichas comunicaciones se identifiquen claramente como comerciales, ofertas promocionales o concursos y deberán indicar el nombre de la persona física o jurídica en nombre de la cual se realizan. Nieto Melgarejo, P (2010).

El art. 20.1 de la Ley 34 del 11 de Julio del 2002, "Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico" (LSSICE), señala que si el medio elegido por el prestador para transmitir la comunicación comercial es el correo electrónico, deberá incluir al comienzo del mensaje la palabra "publicidad". La finalidad de esto es la de prevenir al destinatario, y es éste el que decide si continua adelante con el proceso de contratación o lo interrumpe de forma instantánea. Nieto Melgarejo, P (2010).

En relación a esto la ley modelo de la CNUDMI no hace referencia, de esta misma manera tampoco se menciona en la legislación Colombiana, Uruguaya y la legislación Costarricense.

4. Perfección del contrato

Una duda que se presenta, es: cuándo se perfeccionan los contratos realizados por la vía electrónica. Acerca de esto establece Álvarez, M et al. (2005), que como todo contrato el "contrato electrónico" toma forma a partir del consentimiento. La ausencia de fronteras obliga a analizar el lugar de celebración el que a su vez determinará la ley aplicable y la jurisdicción competente en caso de conflicto.

La Convención de Viena de 1998 sobre Compraventa Internacional de Mercaderías establece que el contrato se perfecciona cuando llega al oferente la notificación de la aceptación. En la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, en la Ley Modelo para el Comercio Electrónico y el derecho

comparado, en general, aceptan pacíficamente que el contrato queda perfeccionado en el momento que la aceptación ingresa al sistema informático del oferente. No es necesario que el oferente tenga conocimiento de la aceptación. Basta que ingrese en su esfera de control. Se establece además, la obligación a cargo del oferente de emitir un "acuse de recibo" de la aceptación para dar seguridad a las transacciones comerciales. Álvarez, M et al. (2005).

Plantea Orúe Cruz, J, R (pp. 111, 2003), que toda transacción entre proveedores y consumidores requiere la presencia de dos elementos: oferta y aceptación, lo cual conlleva al desarrollo de dichos elementos como parte importante de las relaciones comerciales, en este caso, de las relaciones comerciales vía electrónica.

4.1 Oferta

Sobre este importante elemento establece Nieto Melgarejo, P (2010) que la oferta es una declaración unilateral de voluntad emitida por una persona y dirigida a otra u otras, en la que se formula el proyecto de contenido de un contrato. Con la oferta, se inicia la celebración del contrato por una de las partes (oferente) y una vez aceptada por la otra parte (aceptante), lo perfecciona.

Orúe Cruz, J, R (pp. 111, 2003) plantea que la oferta es un acto de manifestación de voluntad unilateral dirigido a la perfección de un contrato y que debe comprender dos elementos esenciales: la cosa y el precio, es decir que sin uno de estos elementos no habría oferta alguna.

Respecto a la oferta la Ley modelo de la CNUDMI contempla en su Arto. 11 lo siguiente: "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 sola razón de haberse utilizado en su formación un mensaje de datos".

En cuanto a la legislación Colombiana, en lo relacionado a la oferta, en su Arto. 14, integra el contenido del artículo de la ley modelo de la CNUDMI, el cual ya mencionamos anteriormente.

4.2 . Aceptación

La aceptación es un elemento indispensable para el perfeccionamiento del contrato, manifiesta Orúe Cruz, J, R (pp. 111, 2003), y consiste en una declaración unilateral de voluntad, dirigida al proponente del contrato y que debe comprender dos elementos, también esenciales: dirigida al proponente del contrato y ceñida a los términos de la oferta.

Para Nieto Melgarejo, P (2010) la aceptación es el segundo momento de la celebración del contrato y "por ella entendemos aquella declaración o acto del destinatario de la oferta en que manifiesta su consentimiento o conformidad con ésta, es decir, manifiesta el deseo de concluir el contrato. De este modo, el concurso de la oferta y la aceptación tiene la virtualidad de perfeccionar el contrato mediante la formación del consentimiento".

En relación a esto la ley modelo de la CNUDMI y la legislación Colombiana no hace referencia más que lo que ya mencionamos anteriormente en su Arto. 11 en el caso de la ley modelo y en el Arto. 14 de la ley de Colombia.

Después del breve análisis sobre el nacimiento de un contrato electrónico, puede afirmarse que para que un contrato se forme y se perfeccione hay que tomar en cuenta un sin número de procedimientos a seguir, para que de esta forma tenga plena eficacia y validez jurídica.

5. Para Álvarez, M et al. (2005) las **características principales del contrato electrónico** son las siguientes:

- Las operaciones se realizan a través de medios electrónicos.
- El lugar donde se encuentren las partes resulta irrelevante.
- No queda registro en papel.

- Se reducen considerablemente los tiempos para efectivizar las transacciones.
- Se reducen los intermediarios de distribución.
- Las importaciones no pasan, necesariamente, por las aduanas

6. Principio de equivalencia funcional

Por qué hablar o hacer referencia a este principio. La respuesta es simple: porque dicho principio no es más que el balance de certeza jurídica que se le da a los documentos electrónicos realizados mediante la red.

Torres, A, Y (2009), expresa que se tiene que partir del principio de equivalencia funcional para la regulación de los actos empresariales electrónicos, y plantea que este principio es considerado como la piedra angular del comercio electrónico. De él se derivan las disposiciones fundamentales que regulan esta nueva actividad mercantil.

La doctrina ha definido este principio según Illescas Ortiz, R (pp 41, 2001), quien considera que el significado de la regla de la equivalencia funcional debe formularse de la siguiente manera: *"La función jurídica que en toda su extensión cumple la instrumentación escrita y autógrafa o eventualmente su expresión oral respecto de cualquier acto jurídico, la cumple igualmente su instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, dimensión, alcance y finalidad del acto así instrumentado. La equivalencia funcional, en suma, implica aplicar a los mensajes de datos electrónicos una pauta de no discriminación respecto de las declaraciones de voluntad o ciencia manual, o gestualmente efectuadas por el mismo sujeto".*

La legislación colombiana consagra el principio de la equivalencia funcional entre los documentos escritos y los documentos electrónicos. En el artículo 5º de la LCCE, literalmente se expresa que "No se negará efecto jurídico, validez o fuerza

obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos". Entiéndase por mensaje de datos según Álvarez, M et al. (2005), a "la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama y el telefax".

Plantea Torres, A, Y (2009), que los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley.

Acerca de estos planteamientos, la Ley 34 del 11 de Julio del 2002, "Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico" (LSSICE) de España establece en su artículo 23 que "*Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez".*

Así mismo plantea Torres, A, Y (2009) que la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de la CNUDMI adoptada en el año 2005, se contempló el principio de la neutralidad tecnológica.

Al respecto, la Convención pretende abarcar todas las situaciones de hecho en que la información se genera, archiva o transmite en forma de comunicaciones electrónicas independientemente de la tecnología o del medio que se haya utilizado.

La convención resalta la importancia de los desarrollos tecnológicos y la velocidad de la innovación, por lo que es importante que las legislaciones den cabida a

futuras novedades tecnológicas y evitar que caigan rápidamente en desuso. Se incluye el término novedoso de la neutralidad de medios haciendo referencia a la necesidad de facilitar los medios de comunicación "*sin papel*", previniendo los criterios para que esos medios puedan equipararse a documentos sobre papel.

La Convención sobre Comunicaciones Electrónicas recoge el principio con la misma formulación y estructura del precepto de la Ley Modelo, si bien adaptando su literalidad al contexto y ámbito de aplicación propio de la Convención. El art. 8.1 de ésta establece: "*No se negará validez ni fuerza ejecutoria a una comunicación o a un contrato por la sola razón de que esa comunicación o ese contrato esté en forma de comunicación electrónica"* Torres, A, Y (2009)

En síntesis podemos decir que los contratos electrónicos siempre y cuando se apeguen a la ley van a tener la misma validez y van a proporcionar la misma seguridad jurídica que un contrato realizado o plasmado en papel, sin distinción alguna por el hecho de realizarse por medio de la red, pero hay que tomar en cuenta también, ya que son muy importantes, debido a que proporcionan mayor seguridad jurídica a las contrataciones electrónicas los siguientes aspectos.

7. Acuse de recibo

Anteriormente mencionamos la frase "acuse de recibo" y es que esta es una forma de dar seguridad jurídica a las partes contratantes por medios electrónicos de que el mensaje que ha sido enviado no fue alterado.

La Directiva Europea del Comercio Electrónico, 2000/31, en el artículo 11, le impone al proveedor de servicios que ha recibido un pedido, con carácter de obligatorio, la expedición de un acuse de recibo, en forma inmediata y por vía electrónica.

Nos indica Márquez, J, F, (2002) que La Ley 34 del 11 de Julio del 2002, "Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico" (LSSICE)

española, en su art. 28, bajo el título “Información posterior a la celebración del contrato”, impone al oferente el envío de un acuse de recibo al aceptante, dentro de las 24 horas siguientes a la recepción de la aceptación.

En relación a esto, la ley modelo de la CNUDMI en su Arto. 14 establece todo lo relativo el acuse de recibo y plantea lo siguiente:

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 baste 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".

Por su parte la Ley 527 de 1999 de Colombia, toma de referencia la ley modelo y acoge específicamente de ésta el inciso 2, literal a y b de su Arto. 14, y lo establece en el Arto. 20 y expresa: "Si al enviar o antes de enviar un mensaje de datos, el iniciador solicita o acuerda con el destinatario que se acuse recibo del mensaje de datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

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

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

Si el iniciador ha solicitado o acordado con el destinatario que se acuse recibo del mensaje de datos, y expresamente aquél ha indicado que los efectos del mensaje de datos estarán condicionados a la recepción de un acuse de recibo, se

considerará que el mensaje de datos no ha sido enviado en tanto que no se haya recepcionado el acuse de recibo.

Como puede verse dicha ley sigue paso a paso la ley modelo y establece como una copia fiel dicho enunciado.

8. Confirmación de envío del mensaje

Señala Márquez, J, F, (2002) que otra técnica útil a fin de dotar de seguridad a la contratación electrónica es la confirmación del mensaje enviado.

En este caso se requiere que quien envió el mensaje (por ejemplo la aceptación), remita un nuevo mensaje confirmando el envío del anterior. El receptor, entonces, tendrá menos posibilidades de dudar del primer envío.

Bien se ha dicho que la utilización de la confirmación (así como la del acuse de

recibo), no eliminan la posibilidad de la utilización de un sistema de información ajeno para enviar un mensaje a nombre de otro. Mas la necesidad de la duplicación del mensaje hará, por lo menos, más dificultoso dicho accionar, Márquez, J, F, (2002)

9. Firma

Talavera Silva, V y Torrez Zelaya, A (Agosto 2008, p.p 26), plantean que la firma comprende la manera ordinaria, cotidiana, habitual y sobretodo, muy particular, con la que una persona traza y asocia su identidad, su nombre y apellido por escrito, ello con el fin de arrogarse voluntariamente las responsabilidades inherentes al contenido de lo que suscribe.

La firma manuscrita ha representado y representa aún, el instrumento por excelencia a través del cual la manifestación de voluntad de los sujetos queda legitimada y corroborada. Vemos así que la firma cumple un rol predominante en lo que respecta a la teoría de los aspectos jurídicos, el cual se encuentra determinado y delimitado por las funciones que la firma manuscrita cumple en la celebración de todo acto jurídico con formalidad escrita. Talavera Silva, V y Torrez Zelaya, A (Agosto 2008, p.p 26)

En relación a la firma refiere Reyes Krafft, A, A (2002), que es el conjunto de letras y signos entrelazados, que identifican a la persona que la estampa, con un documento o texto, y plantea también que existen varios tipos de firmas, como por ejemplo:

- Autógrafa: es la que suscribe la persona física con su propia mano y consiste en un conjunto de letras, o bien algún componente de su nombre y a veces el nombre y apellido, aunado a una serie de trazos que pueden abarcar toda gama de evoluciones del instrumento de escritura, que señalan e identifican al sujeto y lo separan de otros, en los documentos que suscribe y es un elemento que refleja permanentemente su voluntad de expresar lo que firma, o de obligarse al tenor del texto que suscribe.
- Mecánica: es la que es impresa con la ayuda de instrumentos mecánicos.

10. Firma Electrónica

10.1 Concepto

En cuanto a la firma electrónica la ley modelo de la CNUDMI sobre firma electrónica establece en relación a la denominación de esta, que se entenderá por firma electrónica a los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados

para identificar al firmante en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos.

La ley No. 43 de Panamá, “Ley Que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos”, establece en relación a la firma electrónica que ésta es “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”.

Davaras, M, A, (1994), refiere en cuanto al concepto de la firma electrónica que ésta es una manera de representación y confirmación de la identidad de un sujeto en el medio electrónico, hecho mediante cualquier proceso también electrónico; ello permite al receptor identificar formalmente a su autor.

Según La Ley No. 59, Ley de firma electrónica de España (2003), La Firma Electrónica es el “conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”.

La ley de la republica uruguaya denomina a la firma electrónica como los “datos en forma electrónica anexos a un documento electrónico o asociados de manera lógica con el mismo, utilizados por el firmante como medio de identificación”.

Nuestro anteproyecto de Ley de Firma Electrónica plantea que “son datos electrónicos integrados en un mensaje de datos o lógicamente asociados a otros datos electrónicos, que puedan ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de datos”.

10.2 Primeros regulaciones de la firma electrónica

Debido al cambio que ha sufrido nuestra sociedad y a la necesidad de regular las relaciones comerciales por la vía electrónica, surge lo que hoy conocemos como firma electrónica y de esta manera los medios tradicionales pierden validez en el mundo electrónico.

Reyes Krafft, A, A (2002) relata que en Mayo de 1995 en los Estados Unidos de América fue emitida la primera ley sobre firmas digitales por el estado de Utah y es conocida como "Utah digital signature act". El comité de seguridad de la información de la división de comercio electrónico, de la American Bar Association, emitió en Agosto de 1996 la "Guía de firmas digitales".

El 15 de Agosto de 1997 en la conferencia nacional de comisionados sobre derecho estatal uniforme, elaboró el borrador de lo que será la "Uniform Electronic Transactions Act" que fue aprobada el 30 de Julio de 1999.

Además, el 30 de Julio del 2000, se emitió la "Electronic Signatures in global and National Commerce Act". Reyes Krafft, A, A (2002)

En argentina en Marzo de 1999 se le encarga a un grupo de juristas mediante una comisión creada por decreto 685/95, la redacción de un proyecto de código civil que también abarcase las materias electrónicas comerciales, en el cual se prevén importantes modificaciones en el tratamiento de los instrumentos. Se mantiene la regla de libertad de forma y se prevé la formación convenida que es obligatoria para las partes bajo pena de invalidez del negocio jurídico. Se reconocen los instrumentos públicos, los instrumentos privados y los instrumentos particulares que son los no firmados.

Lo relevante es que:

- "Se amplía la noción de escrito, de modo que pueda considerarse expresión escrita la que se produce, consta o lee a través de medios electrónicos".

- Se define la firma y se considera satisfecha el requisito de la firma, cuando en los documentos electrónicos se sigue un método que asegure razonablemente la autoría e inalterabilidad del documento.

- Se prevé expresamente la posibilidad de que existan instrumentos públicos digitales". Reyes Krafft, A, A (2002)

Martín Reyes, M, A (2001), manifiesta que el legislador español, en respuesta a la necesidad de ofrecer el uso de la firma electrónica, en condiciones satisfactorias de calidad y seguridad técnica, secundando opciones ya adoptadas por otros Estados de nuestro entorno social y cultural, dictó el Real Decreto-Ley 14/1999, de 17 de septiembre, regulador de la firma electrónica y de los prestadores de servicios de certificación.

Continúa manifestando Martín Reyes, M, A (2001) y dice que las firmas electrónicas podrán ir acompañadas de un certificado expedido por una entidad de servicio de certificación, existiendo dos tipos de certificaciones la ordinaria y la reconocida o certificado reconocido, que será aquél que contenga los requisitos de información descritos en el artículo 8 del Real Decreto-Ley, que podemos clasificar como: subjetivos y objetivos.

11. **Requisitos subjetivos:** estos hacen referencia al sujeto prestador del servicio de certificación y al signatario debiendo constar:

- "La identidad del prestador del servicio de certificación que lo expida.

- Firma electrónica del prestador del servicio de certificación.

- Firma electrónica del signatario por su nombre o apellidos o con seudónimo siempre que conste como tal.

- Indicación de si actúa en nombre propio o por representación".

12. **Requisitos objetivos:** En cuanto a los datos objetivos constará en el certificado:

    - "Su expedición como certificado reconocido.
    - Su código de identificación.
    - La clave pública de verificación de la firma del signatario.
    - Su período de vigencia.
    - Límites de uso.
    - Límites del valor de las transacciones a realizar.
    - Cualquiera otra que se estime conveniente siempre que se consienta por el signatario".

13. Diferencia entre la firma digital y la firma electrónica

En la actualidad se habla de dos términos, los cuales son la firma electrónica y la firma digital. Con un simple vistazo a estas dos expresiones, cualquiera puede decir que son sinónimos. Vigil Gallo, S,A y Vasquez Espinoza, D, A (2009), señalan que no son dos términos que designen el mismo sistema, sino que conllevan diferencias esenciales y plantean que "**La firma digital** es la utilización de un sistema de encriptación asimétrico, en el que existen dos llaves las cuales consisten en una clave privada y una clave que identifica públicamente al particular, de modo que sólo utilizando su clave pública, el interesado podrá desencriptar el mensaje enviado, y por tanto este último será legible". Mientras que la **Firma electrónica** es cualquier símbolo que se utilice como identificador de una persona en un determinado documento, así como en aquel que en su transmisión utilice medios electrónicos. El nombre de una persona escrito al final del documento, o un

símbolo que le identifique, sería una firma electrónica; y la firma digital es por tanto un tipo de firma electrónica.

14. Propósitos de la Firma electrónica

Sarra, A, V (p.p. 369), expresa que la firma electrónica tiene los siguientes propósitos:

14.1 Consentimiento: la firma expresa el consentimiento sobre lo escrito o la intención de asignarle efectos jurídicos. Según Savigny la declaración escrita se hace poniendo el nombre propio debajo de un acto escrito y la firma estable del acto expresa el pensamiento y la voluntad del que lo firma.

14.2 Solemnidad: el hecho de firmar un documento, llama a la reflexión al firmante, respecto del significado jurídico del acto que realiza y en consecuencia, esta solemnidad tiende a evitar la asunción de compromisos de manera inconsciente.

14.3 Prueba: una firma autentica el cuerpo de escritura que precede, al identificar a su signatario.

14.4 Forma: la firma hace en ocasiones la validez de los actos jurídicos que se celebran. Tal es el caso de los actos formales ad solemnitatem, en los que la forma es un requisito inexcusable de su validez.

15. Características de la firma electrónica

Mencionan Vigil Gallo, S, A y Vásquez Espinoza, D, A (2009), como características de la firma electrónica las siguientes:

- Es un conjunto de datos y no es un símbolo, sello o grafía electrónica que sirve para acreditar la autenticidad e integridad de su contenido.
- Se trata de una técnica de identificación del autor o autores del documento electrónico que recoge.
- Los datos de la firma digital pueden formar parte del documento o ir asociados funcionalmente con ellos

16. Claves públicas y privadas

Anónimo (2010), plantea que el funcionamiento de la firma digital requiere que cada certificado disponga de dos claves.

16.1 Clave privada: esta clave se mantiene en secreto. En la guía para la incorporación de la ley modelo de la CNUDMI para las firmas electrónicas (2001) al derecho interno, se establece que la clave privada es la que se utiliza sólo por el firmante para crear la firma numérica.

16.2 Clave pública: esta se da a conocer al interlocutor en la transacción telemática. En relación a esta clave, la guía para la incorporación de la ley modelo de la CNUDMI para las firmas electrónicas (2001) al derecho interno, establece que ésta la conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado pueda verificar la firma numérica.

Este par de claves, pública y privada, están generadas de forma que “lo que una llave cierra, la otra llave lo abre”. Esto es, si envío un mensaje a una persona firmado con su clave pública, sólo ella lo podrá abrir con su clave privada.

17. Firma electrónica avanzada

Mateu de Ros, R. (2004, p.p. 457), designa como firma digital avanzada a la firma que permite la identificación del signatario, y que 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 a éstos.

Talavera Silva, V, M y Tórrez Zelaya, A, L (pp. 25, 2008), plantean que debido a los problemas que causaba el concepto de la firma digital, se expresaban dudas sobre lo apropiado del uso de los términos "avanzada o seguro" para describir técnicas de firmas electrónicas en general, y que debido a que no había una expresión apropiada para solucionar dichos problemas se decidió a utilizar el vocablo avanzada.

Así se sigue utilizando en la legislación uruguaya, y ésta establece en su Arto.2, inciso k, que la firma electrónica avanzada es la firma electrónica que cumple los siguientes requisitos:

1) "Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca.

2) Ser creada por medios que el firmante pueda mantener bajo su exclusivo control.

3) Ser susceptible de verificación por terceros;

4) Estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detectable; y

5) Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma".

A esta expresión en nuestros días en la mayoría de las leyes vigentes que regulan la firma electrónica se le conoce como firma electrónica reconocida, incluyendo nuestro anteproyecto de ley a diferencia de la ley sobre firma electrónica de Uruguay.

Márquez, J.A (2007), menciona que en México, las reformas al Código de Comercio del veintinueve de Agosto del 2003 consignan en el art. 97 los siguientes requisitos para que la firma electrónica se considere “avanzada” o “fiable”:

Artículo 97.

“La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

- Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante; Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante.
- Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma.
- Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma”.

18. Adelantos de la firma electrónica avanzada.

Talavera Silva, V, M y Tórrez Zelaya, A, L (pp. 64, 2008), comentan que si bien es cierto la firma ológrafa tiene la ventajosa propiedad de la fijación física, inmersa dentro de un contenido delimitado por los datos y el formato del texto y es soportado en un material continente, comúnmente el papel, la firma electrónica avanzada, por definición conceptual y tecnológica, integra otras mejorías:

18.1 Autenticación

Puesto que se logra identificar unívoca y nominalmente al firmante mediante su certificado digital reconocido. O sea, consigue un modo irrefutable de crear un

vínculo entre su autor real y el carácter que éste le ha impreso como declaración de voluntad, todo ello contenido en un documento o archivo electrónico firmado.

18.2 Integridad

Porque el mecanismo como tal garantiza matemáticamente la relación directa contenido-firma, de tal forma que cualquier variante producida en los datos, luego de firmados, podrá ser detectada mediante el proceso de verificación de la firma digital.

18.3 No repudio

Del origen, el emisor no podrá absolutamente, en manera alguna, negar haber enviado el mensaje que contiene los datos firmados digitalmente.

18.4 Control de creación

Puesto que se ha generado por medios que el firmante, en principio pudo mantener bajo su control y por un dispositivo seguro de creación de firma.

19. Valor probatorio del documento informático

En relación al valor probatorio del documento informático establece la Ley modelo de la CNUDMI en su Arto. 9 inciso 2, que 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.

Menciona Márquez, J, A (2007) que para valorar su fuerza probatoria, deben atenderse tres circunstancias: la fiabilidad del método empleado, su atribución personal y su accesibilidad para consulta. Se atenderá primordialmente a la

fiabilidad del método en que haya sido generada, archivada, comunicada o conservada dicha información.

La Ley 527 de 1199 de Colombia en su Arto.28 instituye que el uso de una firma digital tendrá la misma fuerza y efectos que una firma manuscrita, si aquella incorpora los siguientes **atributos:**

- "Es única a la persona que la usa
- Es susceptible de ser verificada
- Esta bajo el control exclusivo de la persona que la usa
- Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es inválida
- Esta conforme a las reglamentaciones adoptadas por el gobierno nacional."

La firma electrónica es más compleja que la firma ológrafa y está sujeta a un porcentaje más alto de falsificación y a la realización de fraudes por medio de la misma, pero aun así tal como lo plantean los citados autores, ésta tiene el mismo valor probatorio que la firma realizada de puño y letra.

Por lo que mencionan Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 226, 2002), lo importante radica entonces en que la firma electrónica debe cumplir las mismas funciones que una firma ológrafa, como son:

- "Identificar al autor.
- Dar certeza de la participación de esa persona en el acto de firmar.
- Relacionar a la persona con el contenido del documento."

Anónimo (2010), establece que la firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación

con los datos consignados en documentos escritos, y será admitida como prueba de en juicio.

Así mismo se plantea en el anteproyecto de ley de firma electrónica de nuestro país, en su Arto. 6, que además de ser admitida en los procesos judiciales como prueba, también se admitirá como medio probatorio en los procesos administrativos.

Se menciona también en este mismo artículo los casos en los cuales no podrá utilizarse la firma electrónica. Dichos casos son:

- "Actos jurídicos del derecho de familia;
- actos personalísimos, en general;
- disposiciones por causa de muerte;
- aquellos actos que deban ser realizados bajo las formalidades exigidas por la ley de la materia o por aquellos acuerdos entre las partes".

Si bien es cierto que el presente anteproyecto de ley de firma electrónica de lo único que hace mención es acerca de las entidades, obligaciones etc., no contempla la creación de un registro de firma electrónica que sea de carácter público. Por medio de éste se otorgaría mayor veracidad a las firmas electrónicas plasmadas en un documento certificado.

20. Ventajas de la firma electrónica

Con la firma electrónica pueden realizarse diferentes tipos de transacciones a través de internet sin necesidad de desplazarse, ni hacer largas filas, agilizando los trámites, aumentando la transparencia, lo que se transforma en ahorros significativos de tiempo y dinero. Anónimo (2010)

21. Proyectos

Con la firma electrónica se pueden desarrollar proyectos como los que mencionaremos a continuación dentro de los cuales se encuentran algunos a los que ya hicimos referencia en el capítulo primero de este documento:

- Trámites de gobierno (Gobierno Electrónico).
- Compras públicas.
- Gestión Documental (Cero Papeles).
- Home Banking seguro.
- Dinero Electrónico.
- Balances Electrónicos.
- Trámites judiciales y notariales.
- Comercio Electrónico.
- Facturación Electrónica.
- Contratos Electrónicos.
- Servicios Web.

CAPITULO III.

ENTIDADES DE CERTIFICACIÓN. ASPECTOS GENERALES.

1. DEFINICIONES.

1.1 Entidad de Certificación.

En la ley modelo de la CNUDMI sobre comercio electrónico del 1996 no se establece literalmente lo que es una entidad de certificación, solamente se refiere en su Arto. 10 a la conservación de los mensajes de datos, y en su inciso 3 menciona que toda persona podrá recurrir a los servicios de un tercero para dicha conservación. Consecutivamente la ley modelo de la CNUDMI sobre firmas electrónicas plantea que ese tercero se conoce en general, en la mayoría de las normas y directrices técnicas, como “entidad certificadora”, “prestador de servicios de certificación” o “proveedor de servicios de certificación”

Ya haciendo una interpretación podemos decir que dicha norma aunque no se pronuncia de manera expresa sobre las entidades de certificación, se refiere a éstas como aquel tercero que ayuda a la subsistencia de un documento electrónico.

Para Gutiérrez, S (2010), una entidad de certificación es aquella persona facultada para emitir certificados en relación con las firmas digitales de las personas.

Plantea Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 258, 2002), que las entidades de certificación, son las encargadas entre otras cosas, de facilitar y garantizar las transacciones comerciales por medios electrónicos o medios diferentes a los estipulados en papel e implican un alto grado de confiabilidad, lo que las hace importantes y merecedoras de un control merecido por un ente

público, control que redunda en beneficio de la seguridad jurídica del comercio electrónico.

Es por esto que Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 258-259, 2002), llegan a la conclusión de que las entidades de certificación son personas naturales o jurídicas autorizadas para supervisar la autoría y la autenticidad de un mensaje de datos de uno de sus suscriptores, a través de la verificación de la firma digital, por medio de un proceso de encriptación del cual se expide un certificado.

Habiendo presentado los diferentes conceptos exteriorizados por los autores señalados, puede establecerse que hay una armonización de dichas concepciones, ya que estos tienen un mismo objeto, el de darnos a entender un mismo significado, siendo éste matizado con diferentes palabras.

Así Panamá en su La ley No. 43, "Ley Que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos", expresa que la entidad de certificación es una Persona que emite certificados electrónicos en relación con las firmas electrónicas de las personas, ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos y realiza otras funciones relativas a las firmas electrónicas". Entiéndase como estampado cronológico, según Anónimo (2010), aquéllos que son también conocidos como timestamping y que es un mecanismo en línea que permite demostrar que una información ha existido y no ha sido alterada desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 y está en el registro de estándares de internet. Una autoridad de estampado cronológico actúa como tercera parte de confianza, testificando la existencia de dichos datos electrónicos en una fecha y hora concreta.

Si bien es cierto que dichas entidades de certificación son las que dan valor a los documentos que llevan plasmada una firma digital y que son remitidos por medios electrónicos, hay que mencionar que de acuerdo a la realidad de nuestro país éstas tendrían que prestar servicios que se adecuen a la realidad de las empresas, es

decir, que ofrezcan certificados en dispositivos económicos y que éstos puedan ser usados en cualquier ordenador sin que la empresa tenga que excederse en sus gastos debido a la instalación de nuevas tecnologías.

Cabe mencionar que en cuanto a nuestra legislación, el anteproyecto de ley de firma electrónica no contempla el concepto de entidades de certificación. A lo único que hace referencia es a los proveedores de servicios de certificación, lo cual mencionaremos en el siguiente apartado.

1.2. Certificador o proveedor de servicios.

Atendiendo a los denominados proveedores de servicios de certificación, Vigil Gallo, S, A y Vásquez Espinoza, D, A (2009), aluden al hecho de que siendo la actividad a la que profesionalmente se dedican los prestadores de servicios de certificación una actividad empresarial, es necesario que se constituyan formalmente como sujetos mercantiles, es decir que deben inscribirse en el registro mercantil, entre otras acciones necesarias para actuar de acuerdo a derecho.

Adicionalmente, los prestadores de servicios pueden estar respaldados por una certificación de prestadores de servicios de certificación. Esta certificación es voluntaria y hace constar que el prestador de servicios cumple con los requisitos específicos de los servicios que ofrecen al público, según la ley de industria de España.

La ley modelo de la CNUDMI sobre firmas electrónicas plantea que por “prestador de servicios de certificación”, se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

La Ley 59, Ley de firma electrónica de España (2003), en su Arto 2 numeral 2 retoma el concepto de prestador de servicios de certificación que establece La ley modelo de la CNUDMI sobre firmas electrónicas.

La ley de certificados, firmas digitales y documentos electrónicos, ley No. 8454 de 30 de Agosto del 2005 de Costa Rica, establece que “se entenderá como certificador la persona jurídica pública o privada, nacional o extranjera, que emite certificados digitales y está debidamente autorizada”.

La Ley No. 18.600, “Ley Documento electrónico y Firma electrónica” de Uruguay, la cual fue publicada el 5 de Noviembre del 2009, alude a dos tipos de prestadores de servicios:

- Prestador de servicios de certificación: persona física o jurídica, pública o privada, nacional o extranjera, que expida certificados electrónicos o preste otros servicios de certificación en relación con la firma electrónica.
- Prestador de servicios de certificación acreditado: aquel prestador de servicios de certificación acreditado ante la Unidad de Certificación Electrónica.

En el anteproyecto de ley de nuestro país, ley de Firma electrónica, (Diciembre, 2005), en su Arto. 3, inciso “e", establece que certificador es la entidad proveedora de servicios de certificación de firma electrónica y en el inciso “r”, menciona el concepto de proveedor de servicios de certificación y plantea que estas son entidades que otorgan, registran, mantienen y publican los certificados de firma electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas y que pueden prestar otros servicios relacionados con la firma electrónica.

Por su parte, Colombia a esto no le da ningún significado, ya que no se encuentra determinado dicho concepto en su Ley 527 sobre firma electrónica.

Pese a esto, podemos señalar que existen similitudes en cuanto a los conceptos establecidos por cada una de las legislaciones de los distintos países. La diferencia más grande radica en cuanto a la legislación Uruguaya, debido a que establece dos tipos de certificadores o proveedores de servicios. Uno de ellos será aquel que esté

debidamente autorizado por una entidad certificadora y el otro sería el que ofrece los mismos servicios, pero no se encuentra autorizado por ningún ente certificador.

Así como lo mencionamos anteriormente, esta autorización es voluntaria, es decir que no hay ningún tipo de imposición para que dichos certificadores soliciten la autorización de una entidad de certificación. Si bien es cierto que dicha autorización no es obligatoria, ésta les permite proporcionar mayor confianza a sus clientes en cuanto a los servicios prestados.

Reyes Ruiz, J, B (2009), denomina a los certificadores o prestadores de servicios de certificación como emisores de certificados y plantea que cualquier individuo o institución, puede generar un certificado digital, pero si este emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por ello los emisores deben acreditarse: así se denomina al proceso por el cual entidades reconocidas, generalmente públicas, otorgan validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados emitidos por la citada institución.

Este autor a pesar de darle nombres diferente a los certificadores, los establece con el mismo concepto, solamente que lo plasma en palabras diferentes, y hace mención también a lo que ya nos referimos anteriormente sobre la fiabilidad que obtiene un certificador cuando está autorizado por una entidad de certificación.

2. Diferencia entre las entidades de certificación y los proveedores de servicios de certificación.

Es importante, con el objetivo de que no haya confusión en relación a lo que se conoce como entidad de certificación y a los proveedores de servicios de certificación, establecer la diferencia que existe entre estos elementos.

Según lo investigado, una entidad de certificación es aquella que autoriza y emite certificados tanto a personas naturales como jurídicas, mientras que los llamados proveedores de servicios de certificación son aquellas entidades públicas o privadas que prestan sus servicios a particulares, dando mayor seguridad a sus relaciones comerciales por medio de los certificados que les fueron emitidos por parte de una entidad certificadora.

Es significativo mencionar que cada entidad de certificación según sea el país en que se encuentre, tendrá que contar con un ente que regule sus actuaciones, por lo que se expondrá cuál es el ente regulador en algunos países.

En el caso de Costa Rica la Ley 8454 "Ley de certificados, firmas digitales y documentos electrónicos" publicada el 30 de Agosto del 2005, establece en su Arto. 23 que el ente administrador y supervisor del sistema de certificación será la Dirección de Certificadores de firma digital, la cual pertenecerá al Ministerio de Ciencia y Tecnología.

En Colombia la Ley No. 527, "Ley del Comercio Electrónico y de las firmas digitales", publicada en 1999 en cuanto al ente rector, en su Arto. 41 establece que la Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación.

La Ley No. 18.600, de Uruguay "Ley Documento electrónico y Firma electrónica" publicada el 5 de Noviembre del 2009 establece en su Arto. 15: desígnese a la Agencia para el Desarrollo del Gobierno de Gestión electrónica y la Sociedad de la Información y el conocimiento como autoridad certificadora a raíz nacional, esta fue según lo dispuesto en este mismo Arto. párrafo primero, la primera autoridad de la cadena de certificación a la cual le compete emitir, distribuir, revocar y administrar los certificados de los prestadores de servicio de certificación acreditados.

En Nicaragua en cuanto a la entidad que regulará el proceso de acreditación de firma electrónica en nuestro país, el anteproyecto de firma electrónica designa a la

Dirección General de Tecnología, (DGTEC), la cual depende del Ministerio de Hacienda y Crédito Público.

Esto parecerá nuevo, y es que efectivamente es algo novedoso, debido a que en el momento en que dicho anteproyecto pasó a la Asamblea Nacional para sus respectivos procesos y llegar así a convertirse en Ley, se le hicieron cambios como éste, ya que anteriormente en el anteproyecto presentado originalmente por el CONICYT el ente escogido para la regulación del proceso de acreditación de firma electrónica rector fue la Dirección de acreditación de Firma Electrónica (DAFE).

3. Finalidad de las entidades de certificación.

Muñoz Esquivel, O (2001) establece que las entidades de certificación tienen como fin primordial garantizar el principio de equivalencia funcional de los mensajes electrónicos de datos cara a cara a los documentos tradicionales o en papel. Para tales fines, las entidades de certificación efectúan un proceso de validación o autenticación de la identidad de los emisores y receptores que envían o reciben los mensajes firmados digitalmente. Dicho proceso opera de la siguiente forma: a través de un sistema de criptografía digital (Public Key Infrastructure) que utiliza dos claves expedidas por la entidad de certificación, una pública y una privada, el receptor del mensaje conoce de manera indubitable que el emisor del mismo es realmente quien dice ser y que éste, a su vez, posteriormente no puede negar el envío de un mensaje electrónico de datos. Adicionalmente, como parte de sus funciones, las entidades de certificación mantienen un registro y estampado cronológico en la transmisión y recepción de los mensajes de datos, lo que permite verificar que un mensaje de datos ha sido efectivamente enviado por su emisor y recibido por su destinatario.

4. Existencia de las entidades de certificación.

Según la doctrina existen tres teorías que explican la existencia de las entidades de certificación.

Es Muñoz Esquivel, O (2001), quien plantea que según la doctrina existen tres teorías sobre la existencia de las llamadas entidades de certificación, las cuales se mencionan a continuación.

4.1 Teoría publicista

Muñoz Esquivel, O (2001) cita al autor chileno Renato Jijena Leiva, quien plantea que la existencia de las entidades de certificación en el marco del comercio electrónico obedece a la necesidad de un mecanismo de resguarde del principio jurídico de "*fe pública*". Parafraseando al jurista uruguayo Couture, Jijena Leiva define el principio de "*fe pública*" como la calidad particular de ciertos documentos que consiste o depende no sólo de la autoridad moral y técnica de quien los ha elaborado, sino también en una ficción legal de que lo aseverado por una entidad facultada para hacerlo, es verdad. Desde esta perspectiva, la función de las entidades de certificación se asemeja a la función fedal otorgada a los notarios. En Nicaragua nuestra Ley del notariado en su capítulo uno, Arto. 2 expresamente dice: "El notariado es la institución en que las leyes depositan la fe pública, para garantía, seguridad y perpetua constancia de los contratos y disposiciones entre vivos y por causa de muerte". Sin embargo, el mismo autor reconoce que sería un gran error encomendar el trabajo de otorgar certificados digitales a entidades o funcionarios auxiliares de la administración de justicia como los notarios, que apenas manejan procesadores de textos o programas de bases de datos o de informática registral.

4.2 Teoría privatista

Esta postura sostiene que la actividad de las entidades de certificación no ha de estar sujeta a autorización previa por parte del Estado. Por el contrario, las mismas se rigen simplemente por las reglas del mercado, esto es, con base en un régimen de libre competencia. Muñoz Esquivel, O (2001)

4.3 Teoría Ecléctica

Muñoz Esquivel, O (2001), plantea que en vez de otorgar una categoría jurídica específica a la actividad certificadora, dicha postura reconoce de la semejanza con la función notarial, destacando su importante contenido técnico. Sin embargo, dicha postura refleja en sí misma una marcada tendencia publicista por cuanto permite que la función certificadora sea reglamentada por el Estado.

Añade Muñoz que lo que dio origen a esta teoría fue una demanda de inconstitucionalidad promovida en Colombia por un grupo de notarios en contra de la Ley 527 del 18 de agosto de 1999, mediante la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. El principal argumento utilizado por los demandantes fue que las funciones de las entidades de certificación estarían dando "*fe pública*" en Colombia, cuando esta función estaba reservada constitucionalmente de manera exclusiva a los notarios, según su entendimiento del artículo 131 de la Constitución Colombiana. Por su parte, quienes defendían la constitucionalidad de la función de las entidades de certificación sostenían que "*ni el comercio electrónico ni la actividad de las entidades de certificación son un servicio público, pues las partes no se encuentran en la obligación ni en la necesidad de solicitar los servicios de una entidad de certificación para la celebración de un negocio jurídico*". De igual manera señalaban que de considerarse como un "*servicio público*", dicha categorización no afectaba su constitucionalidad, debido a que en Colombia la Constitución permite que los particulares puedan prestar un servicio público.

Aquí señalamos a los encargados de autorizar la creación de una autoridad de certificación o prestador de servicios de certificación de algunos países. Son los siguientes:

- En Guatemala, la Superintendencia de Administración Tributaria (SAT), el Registro General de la Propiedad, el Registro Mercantil y el Archivo General de Protocolos.

- En Chile, el Ministerio de Economía.
- En España: la Fábrica Nacional de Moneda y Timbre, el Ministerio de Industria, Turismo y Comercio, la Agencia Catalana de Certificación de la Comunidad y Autoridad de Certificación de la Comunidad Valenciana.
- En Venezuela, la SUSCERTE-MCT (Superintendencia de Servicios de Certificación Electrónica).
- En Perú, el INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual).
- En la República Dominicana el Indotel (Instituto Dominicano de las Telecomunicaciones).
- En Colombia, Certicámara (Sociedad Cameral de Certificación Digital Certicámara, S.A.)
- En México, la Secretaria de Economía. Reyes Ruiz, J, B (2009)

5. En la doctrina, Cuervo, J (S.F), establece que las **funciones de las entidades de certificación** son las siguientes:

- Generación y registro de claves.
- Identificación de peticionarios de certificados.
- Emisión de certificados.
- Almacenamiento en la autoridad de certificación de su clave privada.
- Mantenimiento de claves vigentes irrevocadas.
- Servicios de directorio.

Hablando de las funciones que cada una de las entidades de certificación debe cumplir, no se hace referencia a éstas en ninguna de las legislaciones de Costa Rica, Colombia, Uruguay ni en nuestro propio anteproyecto de ley de firma electrónica.

6. La Comisión Europea distingue entre:

6.1 Autoridades de certificación (AC)

El cometido esencial es "autenticar la propiedad y las características de una clave pública, de manera que resulte digna de confianza, y expedir certificados".

6.2 Terceros de confianza (TC)

Ofrecen diversos servicios, pudiendo gozar de acceso legítimo a claves de cifrado. Un TC podría actuar como una AC.

Lo que la Comisión pretende es que las legislaciones sobre firma digital y AC/TC de los distintos países miembros:

- Se basen en criterios comunitarios.
- Delimiten las tareas -certificación o administración de claves- y servicios.
- Puedan establecerse prescripciones técnicas comunes para los productos de firma digital, en caso de que las disposiciones nacionales no se reconozcan mutuamente y ello merme el buen funcionamiento del mercado interio.r
- Normas claras en materia de responsabilidades (usuarios frente a AC) errores, etc. Cuervo, J (S.F).

7. Clases de Entidades de Certificación.

Si bien es cierto que no existe un capítulo o artículo que contemple directamente las clases de entidades de certificación, se observa que la ley modelo de la CNUDMI sobre firmas electrónicas, formula que las entidades certificadoras podrán ser entidades públicas o privadas. En algunos países, por razones de orden público, se prevé que sólo las entidades públicas estén autorizadas para actuar como entidades certificadoras.

En otros países, se considera que los servicios de certificación deben quedar abiertos a la competencia del sector privado.

En el Arto. 29 de la Ley 527 de Colombia se indica de igual manera que éstas podrán ser públicas o privadas, mientras que en las reglamentaciones anteriores e incluso en nuestro anteproyecto de ley no se establece ninguna disposición sobre esto, es decir que la legislación colombiana se apega una vez más a lo establecido en la mencionada ley modelo.

Aquí mencionamos los tipos de entidades existentes según la doctrina.

7.1 Públicas o privadas

Al igual que en las legislaciones a las cuales hicimos referencia anteriormente en la doctrina se establecen las entidades públicas o privadas y en relación a esto Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 259, 2002), mencionan que la ley es clara y no limita la clase de personas jurídicas que pueden constituirse como entidades de certificación, puesto que pueden ser entidades públicas o privadas dependiendo del origen de los capitales con que éstas sean configuradas. Añaden también que el estado en cualquier momento puede entrar a competir con los particulares por el gran porcentaje monetario que ingresaría a sus instalaciones.

7.1.1 Ejemplos de entidades públicas de certificación

La estructura y el cuadro de funcionamiento de las autoridades de certificación (*public key infrastructure)* prevén generalmente una estructura jerarquizada a dos

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

En España se ha establecido el Proyecto CERES, en el que participan el MAP, el Consejo Superior de Informática, el Ministerio de Economía y Hacienda y Correos y Telégrafos, y contempla el papel de la Fábrica Nacional de Moneda y Timbre como entidad encargada de prestar servicios que garanticen la seguridad y validez de la emisión y recepción de comunicaciones y documentos por medios electrónicos, informáticos y telemáticos.

Se pretende garantizar la seguridad y la validez en la emisión y recepción de comunicaciones y documentos por medios electrónicos, informáticos y telemáticos en las relaciones entre órganos de la Administración General del Estado y otras Administraciones, y entre éstos y los ciudadanos, siguiendo directrices de legislación previa (Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, de 1.992, y Real Decreto 263/1996).

El objetivo de esta autoridad de certificación, con la que otras entidades comerciales de certificación deberán interoperar, requiere el reconocimiento de todos los efectos legales del certificado digital.

Los servicios que están previstos a ofrecer son:

- Primarios: Emisión de certificados, archivo de certificados, generación de claves, archivo de claves, registro de hechos auditables.
- Interactivos: Registro de usuarios y entidades, revocación de certificados, publicación de políticas y estándares, publicación de certificados, publicación de listas de revocación y directorio seguro de certificados.
- De certificación de mensajes y transacciones: Certificación temporal, certificación de contenido, mecanismos de no-repudio: confirmación de envío y confirmación de recepción.

- De confidencialidad: Soporte de mecanismos de confidencialidad, agente de recuperación de claves y recuperación de datos protegidos.

7.1.2 En cuanto a las autoridades privadas de certificación están las siguientes.

En España existen focos privados de actividad vinculados con la confiabilidad, el más significativo es el denominado ACE (Agencia de Certificación Electrónica) que está formado por CECA, SERMEPA, Sistemas 4B y Telefónica, y es una Autoridad de Certificación corporativa del sistema financiero español.

También existe como Terceros de confianza el Banesto.

En Bélgica existe el Tercero Certificador llamado Systèeme Isabel, que ofrece servicios certificadores a socios financieros y comerciales.

La Cámara de Comercio unida a la empresa Belsign ha formado un Trusted Third Party en el cual la Cámara de Comercio hace las funciones de Registro y Belsign hace las funciones notariales.

En Estados Unidos existe el Utah Digital Signature Trust, One So. Main, Salt Lake City, Utah y ARCANVS, S.A. Sanders Lane, Kaysville, Utah.

7.2 Por su origen nacional o extranjero

A raíz de la globalización, y en especial a todo lo relacionado con las comunicaciones, se permite que quienes estén interesados en asumir este tipo de actividades lo puedan hacer sin tener en cuenta su nacionalidad, solamente con el cumplimiento de los requisitos establecidos en la ley. Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 259, 2002).

Es decir que no hay ninguna discriminación por el hecho de no ser nacional de un determinado país. Solamente hay que seguir las normativas para poder constituirse como una entidad de certificación.

7.3 Entidades de certificación abiertas y cerradas

7.3.1 Cerradas

El decreto 1747 del 2000 de Colombia, en su Arto. 1 establece que las entidades de certificación cerradas son las que ofrecen servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor sin exigir remuneración por ello.

Respecto a esta definición Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 262, 2002), explican que las entidades de certificación cerradas son aquellas que realizan sus actividades exclusivamente con un suscriptor. Por ejemplo, el caso de una entidad que suministra su propio sistema de certificación con relación a un usuario determinado. Por lo tanto, la relación solo existe entre la entidad y el usuario, con el requisito de ser gratuitas.

7.3.2 Abiertas

Acerca de este tipo de entidades de certificación, Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 263, 2002), mencionan que éstas siempre son de carácter oneroso, y su relación contrario sensu, no abarca exclusivamente una relación entre dos partes, sino que hay una multilateralidad de partes.

En cuanto a este tipo de entidades, lo único que nos queda por decir es que una es de carácter oneroso y en ellas se relacionan varias partes, mientras que la otra es de carácter gratuito y solo existe una relación entre el usuario y el certificador.

8 Naturaleza jurídica de las entidades de certificación.

En relación a la naturaleza jurídica de las entidades de certificación, lo cual ha sido bastante difícil de esclarecer, Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 269, 2002), hacen dos anotaciones las cual son consideradas importantes y plantean:

- “La función pública, tomada en un sentido amplio, designa al conjunto de regímenes aplicable a la generalidad del personal de la administración”.

Empero, cuando se refiere al servicio público y en especial al que presta la entidad de certificación, se trata de una entidad catalogable como comercial, y hay que tener en cuenta que son aquellos que aparecieron en ocasión de la crisis de la noción de servicio público tradicional, que corresponden a actividades que habitualmente han sido consideradas más propias de los particulares que del estado, por lo cual, a pesar de aparecer ahí el elemento de interés general, se ejercen al mismo tiempo con un criterio de beneficio particular que se traduce en el ánimo de lucro. Uno de los ejemplos que dan estos autores son los servicios públicos de transporte.

- La segunda posición que mencionan, es de que se trata de un servicio público, el cual para ellos se adecúa perfectamente al desarrollo de la actividad, pues se entiende como servicio público: "toda actividad organizada que tiende a satisfacer necesidades de interés general en forma regular y continua, de acuerdo con un régimen jurídico especial, bien que se realice por el estado directa o indirectamente o por personas privadas".

Por estos planteamientos es que logramos determinar que la naturaleza jurídica de las mencionadas entidades de certificación no está muy clara, ya que según diferentes legislaciones se les atribuye naturaleza pública o privada. Pública debido a que el estado es quien vendría a regir el funcionamiento de las entidades de certificación, incluso no sólo el hecho de autorizar su funcionamiento, sino como bien lo decía Cuervo, que actuaría como un proveedor de servicios de certificación. También se enfatiza en la palabra entidad, ya que en algunas legislaciones se usa este vocablo, lo cual puede crear confusión debido a que algunos pueden alegar que al denominar a dichas entidades como autoridad de certificación se está haciendo mención a un órgano del estado. En el caso de que sean entes ajenos al estado, es decir que sean los particulares los que vayan a actuar como entidades certificadoras, se va a entender que son de carácter privado.

Debido a que existen tanto entidades de certificación públicas como privadas es que se ha llegado a la conclusión de que la naturaleza jurídica de las entidades de certificación es mixta.

9 Obligaciones de un proveedor de servicios de certificación

Dichas obligaciones de los proveedores de servicios de certificación, no se mencionan ni en la legislación costarricense, ni en la colombiana, mientras que la ley uruguaya establece los que mencionaremos a continuación. Por su parte, nuestro anteproyecto de ley no se queda corto y estipula cuáles serán las obligaciones de un proveedor de servicios de certificación.

Se contemplan en la Ley de Uruguay, Ley Nº 18.600, documento electrónico y firma electrónica como obligaciones de servicios de certificación los siguientes:

1) Abstenerse de generar, exigir, o por cualquier otro medio, tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma electrónica avanzada de los titulares de los certificados reconocidos por él emitidos.

2) Proporcionar al solicitante antes de la expedición del certificado reconocido la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

a) Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica avanzada, que sean compatibles con los datos de firma y con el certificado reconocido expedido.

b) Los mecanismos para garantizar la fiabilidad de la firma electrónica avanzada de un documento a lo largo del tiempo.

c) El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado reconocido.

d) Las condiciones precisas de utilización del certificado reconocido, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

e) Las acreditaciones que haya obtenido el prestador de servicios de certificación.

f) Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados reconocidos deberá estar disponible a instancia de éstos.

3) Mantener un registro actualizado de certificados reconocidos en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del registro se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

4) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados reconocidos.

5) Informar a la Unidad de Certificación Electrónica, cualquier modificación de las condiciones que permitieron su acreditación durante la vigencia de su inscripción en el Registro de Prestadores de Servicios de Certificación Acreditados.

En relación a dichas obligaciones, nuestro anteproyecto de ley de firma electrónica, contemplados en su Arto. 21 menciona los siguientes:

1. Garantizar la utilización de un servicio expedito, seguro de guías de usuario y de un servicio de revocación seguro e inmediato.

2. Garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado.

3. Comprobar, de conformidad con la legislación correspondiente, la identidad y, si procede cuales quiera atributos específicos de la persona a la que se expide un certificado reconocido.

4. Contratar un seguro apropiado para responder por los daños y perjuicios que ocasione ante el titular de la firma electrónica o ante terceros.

5. Registrar toda la información pertinente relativa a un certificado reconocido durante un periodo de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos.

6. 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, incluido 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, ante notario público con cinco años de experiencia profesional. 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.

7. Utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

    7.1 Sólo personas autorizadas puedan hacer anotaciones y modificaciones.

    7.2 Pueda comprobarse la autenticidad de la información.

7.3 Los certificados estén a disposición del público para su consulta solo en los casos en los que se haya obtenido el consentimiento del titular del certificado.

7.4 El agente pueda detectar todos los cambios que pongan en entre dicho los requisitos de seguridad mencionados.

Haciendo una breve comparación entre dichas legislaciones en uno que otro inciso de éstas, podemos observar que existen semejanzas en cuanto a lo planteado anteriormente. Por ejemplo se observa que el numeral 2, inciso c de la ley de Uruguay, es similar al contenido del numeral 3 de nuestro anteproyecto de ley.

La ley modelo de la CNUDMI hace también referencia a las obligaciones de un prestador de servicios de certificación y plantea que "la obligación general del prestador de servicios de certificación es utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables y actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas. Además, se espera que actúe con diligencia razonable para cerciorarse de que todas las declaraciones materiales que haya hecho en relación con el certificado sean exactas y cabales. En el certificado, el prestador deberá proporcionar información fundamental que permita al tercero que haya de confiar en el certificado, determinar la identidad del prestador de servicios de certificación.

También deberá permitir determinar:

a) Que la persona nombrada en el certificado tenía bajo su control los datos en la fecha en que se emitió el certificado; y *b)* que esos datos eran válidos en la fecha en que se emitió el certificado o antes de ella. Con respecto al tercero que ha de confiar, el prestador de servicios de certificación deberá aportar también información relativa a: *a)* el método utilizado para identificar al firmante; *b)* cualquier limitación en los fines o el valor respecto de los cuales pueda utilizarse el dispositivo de creación de la firma o el certificado; *c)* las condiciones de funcionamiento del dispositivo de creación de la firma; *d)* cualquier limitación en

cuanto al ámbito o el alcance de la responsabilidad del prestador de los servicios de certificación; *e)* si existe un medio para que el firmante dé aviso de que un dispositivo de creación de firma ha quedado en entredicho; y *f)* si se ofrece un servicio de revocación oportuna del certificado".

10 Requisitos para ser proveedor de servicios de certificación

La entidad de certificación debe de reunir los requisitos que determine la ley, conocimientos técnicos y experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad. Se debería prever el caso de desaparición del organismo certificador y crear algún registro general de certificación tanto nacional como internacional, que a su vez auditase a las entidades encargadas, y fuese garante de su funcionamiento.

En la legislación sobre firma electrónica de Costa Rica, no encontramos establecidos los requisitos que deberá seguir una persona para llegar a constituirse en un proveedor de servicios. Igualmente en Colombia, mientras que por su parte en Uruguay y en nuestro anteproyecto de ley, sí se plantean dichos requisitos.

Según la legislación Uruguaya son los siguientes:

1. Ser persona física o jurídica constituida en el país, dar garantía económica y solvencia suficiente para prestar los servicios.
2. Contar con personal calificado con conocimiento y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica avanzada.
3. Utilizar estándares y herramientas adecuadas según lo establecido por la Unidad de Certificación Electrónica.

4. Estar domiciliado en el territorio de la República Oriental del Uruguay, entendiéndose que cumple con este requisito, cuando su infraestructura tecnológica y demás recursos materiales y humanos se encuentren situados en territorio uruguayo.

En nuestro anteproyecto de ley de firma electrónica, se contemplan dichos requisitos en su Arto. 20:

1. Un establecimiento permanente situado en territorio nicaragüense donde resida de forma continua o habitual, así como de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

2. Emplear personal que tenga los conocimientos especializados, la experiencia y las calificaciones necesarias correspondientes a los servicios prestados, en particular el personal deberá poseer competencia en materia de gestión informática,conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados. Tal personal deberá poner en práctica los procedimientos administrativos y de gestión adecuada y conformes a normas reconocidas internacionalmente.

3. Contar con sistemas y productos fiables que estén protegidos contra toda alteración a fin de garantizar la seguridad jurídica, técnica y criptográfica de los procedimientos con que trabajan y la confidencialidad de la información.

4. Ser persona jurídica debidamente constituida e inscrita en el registro público mercantil.

5. Disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente ley, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, según regulación de la entidad rectora.

6. Contratar a uno o varios notarios públicos con cinco años de experiencia profesional, a fin que puedan dar fe pública sobre el cumplimiento de las

obligaciones del proveedor de servicio en el momento del libramiento del certificado al titular.

Cabe mencionar que también en cuanto a los requisitos encontramos ciertas similitudes en lo establecido en la ley uruguaya y el anteproyecto de nuestro país. Así el numeral 1 de la legislación de Uruguay se relaciona con el numeral 4 y 5 cinco de nuestro anteproyecto; el numeral 2 de la legislación uruguaya se acopla al contenido existente en el numeral 2 del anteproyecto de firma electrónica de Nicaragua, y por último existe relación entre el numeral 4 de Uruguay y el numeral 1 de nuestro anteproyecto de ley.

Es evidente que en nuestro anteproyecto de ley de firma electrónica se exige un mayor número de requisitos para llegar a ser un proveedor de servicios de certificación.

11 Certificados

Plantea Gutiérrez, S (s.f), que un certificado es un mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste.

La ley modelo de la CNUDMI sobre firmas electrónicas, expresa que 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.

Por su parte en Costa Rica, en su ley de certificados, firmas digitales y documentos electrónicos, ley No. 8454 de 30 de Agosto del 2005 plantea lo siguiente en cuanto a los certificados:

Entiéndase por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:

- La vinculación jurídica entre un documento, una firma digital y una persona.

- La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.

- La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.

- Las demás que establezca esta Ley y su Reglamento.

Por su parte La ley No. 43 de Panamá, “Ley que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos” establece que certificado es la 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.

La Ley Nº 18.600 “Documento electrónico y firma electrónica” de Uruguay hace referencia a dos tipos de certificados, y expone lo siguiente:

- Certificado electrónico: documento electrónico firmado electrónicamente que da fe del vínculo entre el firmante titular del certificado y los datos de creación de la firma electrónica.

- Certificado reconocido: certificado electrónico emitido por un prestador de servicios de certificación acreditado.

Aquí nos podemos dar cuenta de que no es lo mismo hablar de certificado electrónico y de certificado electrónico reconocido. Se podría decir que este último es el más adecuado en cuanto a su seguridad y eficacia jurídica, ya que es el emitido por un ente autorizado para hacerlo.

En lo que respecta a nuestro anteproyecto de ley de firma electrónica, éste contempla a diferencia de la ley uruguaya, tres conceptos sobre los certificados:

- **Certificado**: Es la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta.

- **Certificado de firma electrónica:** Es el documento electrónico firmado electrónicamente cuyos datos son vinculados a su titular y suministrado por un proveedor de servicios de certificación.

- **Certificado digital:** Certificación electrónica que da fe sobre los datos que identifican a quien posee la llave pública suscrita en el certificado digital.

A nuestro entender estos certificados son los que identifican, el primero a la persona como tal, es decir es aquel que hace constar que una persona determinada es el titular de esa firma; el segundo, aquel en el que se plasma la información de una persona, no solamente la firma como tal, y hace constar que esa información pertenece a ésta por medio de la autorización de un proveedor de servicios de certificación y que es con la cual realizará sus transacciones electrónica. Por último, el certificado digital viene siendo aquel que da certeza de los datos contenidos en el certificado como tal.

La ley costarricense solamente contempla los certificados digitales establecidos, como mencionamos anteriormente en nuestro anteproyecto de ley. En cambio en la ley 527 del Dieciocho de Agosto de 1999 de Colombia, no se menciona lo de los certificados emitidos por una entidad de certificación.

12 Para Cuervo, J (S.F) las autoridades de Certificación pueden emitir **diferentes tipos de certificados:**

- Los certificados de Identidad, que son los más utilizados actualmente dentro de los criptosistemas de clave pública y que ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.

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

- Los Certificados Transaccionales son 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.

En relación a esto, la legislación uruguaya establece dos tipos de certificados, los certificados electrónicos y los certificados reconocidos, los cuales ya fueron explicados anteriormente.

Así también explicamos los que se contemplan en nuestro anteproyecto de ley, los cuales son tres: certificado de firma electrónica, certificado digital y el certificado como tal.

13 Plantea Echenique Castellanos de Ubao, L, G (S.F), que **El certificado se caracteriza por lo siguiente:**

- El soporte no es físico, sino electrónico.
- Tiene por misión vincular los datos que resultan de la verificación de una firma a su autor o signatario.
- También confirma la identidad del signatario, es decir, acredita que el mensaje telemático ha sido escrito y enviado por la persona que aparece como signatario y no por otra distinta. Esta función es fruto del sistema de claves públicas y privadas y, en su caso, posteriores códigos, que los intervinientes en el proceso de comunicación deben introducir para que éste tenga lugar.

14 Según la Ley 59/2003 de España en su Arto. 8 se establecen **las causas de extinción de la vigencia de un certificado electrónico. Éstas son:**

- La expiración del período de validez que figura en el certificado.
- La revocación formulada por el firmante, la persona física o jurídica representada por éste, o un tercero autorizado, o la persona física solicitante de un certificado electrónico de persona jurídica.
- La violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación, o la utilización indebida de dichos datos por un tercero.
- La resolución judicial o administrativa que lo ordene.
- El fallecimiento o extinción de la personalidad jurídica del firmante; el fallecimiento o extinción de la personalidad jurídica del representado; la incapacidad sobrevenida, total o parcial, del firmante o de su representado; la terminación de la representación; la disolución de la persona jurídica representada o la alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- El cese en su actividad del prestador de servicios de certificación, salvo que, previo consentimiento expreso del firmante, la gestión de los certificados expedidos por él sean transferidos a otro prestador de servicios de certificación.
- La alteración de los datos aportados para la obtención del certificado o la modificación de las circunstancias verificadas para la obtención del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- Cualquier causa lícita prevista en la declaración de prácticas de certificación.

La legislación de Uruguay establece un sin número de puntos por medio de los cuales se puede extinguir la vigencia de un certificado, siendo estos los mismos establecidos en la ley 59/2003 de España. La única diferencia radica en la forma en

que algunos de ellos fueron redactados. Son diferencias meramente formales y no de fondo.

En lo que respecta a esto, nuestro anteproyecto de ley de firma electrónica, incluye en su Arto. 7, cinco de los puntos señalados anteriormente contenidos en la Ley 59/2003 de España, estos son:

- A solicitud de su titular
- Fallecimiento o incapacidad definitiva de su titular
- Por cese de la actividad del proveedor de servicios de certificación, en el caso de la firma electrónica certificada.
- Disolución o liquidación de la persona jurídica, titular de la firma.
- Por causa judicial que así lo declare.

Por su parte Costa Rica no hace mención a la extinción, pero si contempla la revocación de dichos certificados y plantea que el certificado digital será revocado en los siguientes supuestos:

- A petición del usuario, en favor de quien se expidió.
- Cuando se confirme que el usuario ha comprometido su confiabilidad, desatendido los lineamientos de seguridad establecidos, suplido información falsa al certificador u omitido otra información relevante, con el propósito de obtener o renovar el certificado.
- Por fallecimiento, ausencia legalmente declarada, interdicción o insolvencia del usuario persona física, o por cese de actividades, quiebra o liquidación, en el caso de las personas jurídicas.
- Por orden de la autoridad judicial o cuando recaiga condena firme contra el usuario, por delitos en cuya comisión se haya utilizado la firma digital.

De igual manera la Ley No. 527 de Colombia, “Ley del Comercio Electrónico y de las firmas digitales”, publicada en 1999, se pronuncia sobre la revocación de un certificado y menciona que en dicha ley se establecen dos supuestos en los cuales se puede dar la revocación de un certificado:

Primero: el suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:

- Por pérdida de la clave privada.
- La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

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

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

- A petición del suscriptor o un tercero en su nombre y representación.
- Por muerte del suscriptor.
- Por liquidación del suscriptor en el caso de las personas jurídicas.
- Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
- La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
- Por el cese de actividades de la entidad de certificación.

- Por orden judicial o de entidad administrativa competente.

En cuanto a la extinción de la vigencia de un certificado, la ley modelo de la CNUDMI sobre firmas electrónicas no hace referencia, así como tampoco se pronuncia específicamente sobre la revocación de éstos, solamente menciona que se puede realizar la revocación pero no estipula dichos supuestos de manera taxativa.

15 Características de los contratos de certificación.

Cabe mencionar que dichos contratos son aquellos que se realizan entre la entidad de certificación y el usuario de los servicios de dicha entidad.

Estipulan Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 293-294, 2002), que las características de los contratos de certificación son las siguientes:

15.1 Estrecha relación con la estructura técnica

El desarrollo de la actividad certificadora está sumergida necesariamente en el contorno técnico del momento, pues como es de conocimiento general, el desarrollo respecto a softward y a hardward en la actualidad es muy rápido y ágil, de modo que una entidad de certificación, para que pueda estar al nivel de los avances tecnológicos, debe de gozar dentro de su infraestructura de la tecnología de punta en el área en el que se desarrolla.

15.2 Carácter personalísimo

La actividad que se presta por parte de la entidad certificadora, está basada en la celebración de contrato intuito personae y por lo tanto se requiere el cumplimiento de requisitos especiales de ambas partes.

15.3 Buena fe

En este sentido es esencial para el contrato de certificación, el principio de la buena fe, el cual no se limita a la relación de los co-contratantes pues se ha de entender en sentido amplio, habida cuenta que se encuentra la comunidad involucrada con el desarrollo de la actividad, y más aún con la certeza jurídica que brinda seguridad jurídica a los negocios que se celebran en este medio.

15.4 Adhesivos

A raíz de las características mismas del contrato de certificación es necesario que sean contratos de adhesión ante la imposibilidad de negociar con cada suscriptor las condiciones en que se celebra el contrato, de modo que la autonomía de la voluntad en gran medida se ve limitada en aras de la sensatez

16 Interacción de las entidades de certificación y firma electrónica como elemento importante en el comercio electrónico.

Habría que apuntar los agentes y operadores que interactúan en el comercio electrónico, dentro de los cuales encontramos como puntos indispensables a las llamadas entidades de certificación y a la firma electrónica, los cuales juegan un papel de suma importancia en las relaciones comerciales que se realizan por la vía electrónica.

En el caso del comercio electrónico plantea López Pulido, J, P (s.f.), que la autoridad de certificación o proveedor de servicios de certificación, actúa como garante de la autenticación, integridad y confidencialidad de la información, basándose en una infraestructura de claves. Esto conlleva un gran valor en cuanto

a la seguridad que adquiere la compra y venta de productos por medios electrónicos.

En cuanto a lo relacionado con la firma electrónica, el desarrollo del comercio electrónico está indudablemente ligado al uso y al reconocimiento jurídico de ésta, como medio de autenticación electrónica de documentos, lo que permite dotar de un mayor grado de fiabilidad a las transacciones que se realicen por medios electrónicos.

La Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre (por la que se establece un marco comunitario para la firma electrónica, y a la cual se adapta el Anteproyecto de Ley de Firma Electrónica, cuyo borrador es de 27 de diciembre de 2001, que modificará el Real Decreto Ley 14/1999, de 17 de septiembre), pretende crear un marco jurídico comunitario para el reconocimiento de la firma electrónica y para determinados servicios de certificación, con el fin de garantizar el correcto funcionamiento del mercado interior. López Pulido, J, P (s.f.)

17 Auditorías Jurídicas.

Si bien es cierto que en nuestra ley de firma electrónica no se establece lo que es una auditoria, ni los procedimientos con los cuales se realizan éstas, es de suma importancia a nuestro parecer, por lo que a continuación lo establecemos, tal como lo plantea Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 303, 2002).

La Auditoria no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo, son de carácter indudable. Por el contrario, la auditoria es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada, y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

17.1 Objetivos de las auditorias a una entidad de certificación.

Enumeran Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 304, 2002), los siguientes enunciados como objetivos de una auditoría:

- El control de la función informática que consiste en el análisis de los procesos de certificación y protección de la información recaudada.
- El análisis de la eficiencia de los sistemas informáticos que comporta.
- La verificación del cumplimiento de la normativa general de las entidades de certificación con base en los parámetros legales diseñados.
- La revisión de la gestión que está siendo efectuada sobre los recursos materiales y humanos con que cuenta la entidad.

Se deben de tomar en cuenta un sinnúmero de parámetros en la realización de una auditoria a una entidad de certificación, dentro de los cuales son fundamentales los parámetros de confidencialidad y seguridad lógica, pues no se puede llegar a permitir que se den los denominados delitos de cuello blanco, o que se den fenómenos como el llamado virus de computadora.

Expresan Cubillos Velandia, R, y Rincón Cárdenas, E, (pp 317, 2002), que el principal riesgo a eliminar en la actividad certificadora, será el de sabotaje o delitos a través de la red, casos en los cuales los sistemas de prevención acogidos por la empresa serán determinantes para tal cometido.

Otras precauciones que se deben tomar en cuenta al momento de auditar las instalaciones físicas de la empresa serán las siguientes:

- La ubicación de los equipos y la infraestructura tecnológica requerida para la actividad certificadora.
- Los ductos de aire, sea este artificial o natural, se deben encontrar en perfectas condiciones, ya que estos son la principal causa de la acumulación

de polvo e incluso de agua que ante una eventualidad pueden ocasionar trastorno en los equipos.

- La empresa debe contar con detectores de humo, que indiquen la posible presencia de fuego y el mantenimiento de extintores apropiados que no perjudiquen los equipos.

- Las instalaciones deben de contar con un equipo de fuente no interrumpible tanto en los equipos o servidores, como en la red; de igual forma, esto debe estar presente en los equipos de teleprocesos.

- Verificar las prácticas de evacuación del lugar de trabajo ante posibles siniestros, teniendo en cuenta el sistema con el cual se salvaguardará toda la información contenida en la base de datos.

- Verificar la existencia de salidas de emergencia, y que éstas estén debidamente controladas, para evitar hurtos o cualquier clase de contingencia.

En relación a las auditorias, mencionaremos algunas de las legislaciones en las cuales se encuentra estipulado dicho enunciado.

En Costa Rica por ejemplo la Ley 8454 “Ley de certificados, firmas digitales y documentos electrónicos”, publicada el 30 de Agosto del 2005, es expresa al referirse directamente en su Arto. 21 a las auditorías, es decir que dedica un enunciado específico a la realización de éstas, cosa muy importante, ya que éstas como lo plantemos en el desarrollo del presente estudio, tienen como fin evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Dicha ley establece en el mencionado Arto., que todo certificador registrado estará sujeto a los procedimientos de evaluación y auditoría que acuerde efectuar la dirección de certificadores de firma digital o el Ente Costarricense de Acreditación (ECA).

Ley No. 527 de Colombia, “Ley del Comercio Electrónico y de las firmas digitales”, publicada en 1999, pese a que ésta es una de las primeras leyes en contemplar todo lo relacionado a las firmas electrónicas, ya incluía para entonces lo relacionado a las auditorías, y de esta forma en el Arto 32 se mencionan los deberes de las entidades de certificación, dentro de las cuales en su numeral 8, se plantea lo relacionado a las auditorías y expresa que hay que permitir y facilitar su realización por parte de la superintendencia de Industria y Comercio.

Mencionamos también la Ley No. 18.600 de Uruguay, “Ley Documento electrónico y Firma electrónica” publicada el 5 de Noviembre del 2009, por ser una de las más recientes.

En su Arto 14. se plantean las funciones y atribuciones de la unidad de certificación electrónica y en su inciso 2 literal b, establece que se realizarán auditorías a los prestadores de servicios de certificación acreditados, de conformidad con los criterios que la reglamentación establezca para verificar todos los aspectos relacionados con el ciclo de vida de los certificados reconocidos y de sus claves criptográficas.

En cuanto a nuestro Anteproyecto de Ley de Firma electrónica, realizado y propuesto por el Consejo Nicaragüense de Ciencia y Tecnología (CONICYT), se contemplan también las auditorías y otorga un sin número de potestades a la Dirección General de Tecnología (DGTEC), dentro de las cuales se encuentra la realización de auditorías técnicas a los proveedores de servicios de certificación.

La ley modelo de la CNUDMI también se refiere a las auditorías y establece dentro de los elementos como posibles factores a tener en cuenta para determinar el grado de fiabilidad de un prestador de servicios de certificación, el mantenimiento de un registro de auditoría y la realización de auditorías por una entidad independiente.

18 Delitos informáticos.

No se estudiará de lleno lo que son los delitos informáticos, pero sí es de suma importancia hacer una breve referencia a éstos, ya que son los que atacan a los diferentes proyectos que se han creado y que toman vida por medio de la red.

Plantea Chavarría, A, R, Pereira Vega, J, A y Lenin Ernesto Dávila, L, E, que a nivel internacional se considera que no existe una definición propia del delito informático. Sin embargo, muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

A éstos denomina Téllez Valdés, J (2003, p.p. 163), como actos ilícitos en los que se tiene a las computadoras como instrumento o fin.

Agregan Chavarría, A, R, Pereira Vega, J, A y Lenin Ernesto Dávila, L, E, que se entenderán como "delitos informáticos" a todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal que hacen uso indebido de cualquier medio informático.

Y es que la aparición de la llamada *ciberdelincuencia* es un problema que cada día preocupa más a la sociedad de la información, tal como lo plantea López Pulido, J, P (2010), con delitos como el "blanqueado" electrónico de dinero, las actividades de juego ilegal, la piratería informática o la violación de los derechos de la propiedad intelectual, lo cual pone a prueba los actuales sistemas de prevención, descubrimiento y persecución de delitos. La cooperación internacional ya está muy avanzada en determinadas áreas, así como la lucha contra la delincuencia internacional organizada.

Según lo que hemos indagado, a estos delitos también se les conoce como delitos de cuello blanco, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943.

En Europa, y en un contexto internacional más amplio, se han creado grupos especiales y se ha reforzado la cooperación transfronteriza en áreas como la

localización y seguimiento de delincuentes en línea y la búsqueda y confiscación de pruebas digitales.

El Consejo de Europa aprobó (con la firma de 30 estados miembros), el 23 de noviembre de 2001, el Convenio Europeo sobre Cibercrimen. Por su parte, en la Unión Europea y a raíz del Consejo Europeo de Dublín, se creó el Grupo de Alto Nivel, que está ultimando un plan de acción para luchar contra la *ciberdelincuencia*. Estos esfuerzos revisten una importancia fundamental para incrementar la confianza en el comercio electrónico internacional. López Pulido, J, P (2010).

Hay que tener presente que en los delitos cometidos en la Red es preciso determinar el lugar de comisión para establecer cuál es la legislación aplicable y la jurisdicción competente, lo que lleva, casi necesariamente, a tomar en cuenta el país en el que se halla el servidor. López Pulido, J, P (2010).

La tipificación de nuevas modalidades delictivas que implican el uso de redes informáticas, y aquellas otras figuras delictivas *tradicionales* en las que la Red sirve como instrumento de comisión, puede considerarse también un instrumento de prevención de delitos, por lo que, a título meramente indicativo, expone López Pulido, J, P (2010), una de las modalidades delictivas que recoge el Código Penal español de 1995.

Entre los delitos contra la intimidad se tipifica la interceptación del correo electrónico (artículo 197.1), figura delictiva que queda asimilada a la violación de correspondencia, cuando las actividades conducentes a ello se realizan sin consentimiento del afectado y con la intención de descubrir sus secretos y vulnerar su intimidad. López Pulido, J, P (2010).

En nuestro actual Código Penal en su titulo 3, capítulo 1, específicamente no se refiere a los delitos informáticos, pero establece en su **Art. 192 Apertura o interceptación ilegal de comunicaciones "***Quien ilegítimamente abra, intercepte o por cualquier otro medio se entere del contenido de una carta, un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le*

esté dirigido, será penado con prisión de seis meses a dos años. Si además difundiera o revelara el contenido de las comunicaciones señaladas en el párrafo anterior, se impondrá prisión de uno a tres años". Y en su Arto. 1**93 Sustracción, desvío o destrucción de comunicaciones "***Quien sin enterarse de su contenido, se apodere ilegalmente, destruya o desvíe de su destino una comunicación que no le esté dirigida, será penado con prisión de seis meses a un año. Quien conociendo o presuponiendo el contenido de la comunicación realizare la conducta prevista en el párrafo anterior, será penado con prisión de uno a dos años"*

Bajo los auspicios de la Organización Mundial de la Propiedad Intelectual, y con el precedente del Convenio de Berna del 9 de septiembre de 1986 (revisado en París el 24 de julio de 1971), para la protección de las obras literarias y artísticas, se han desarrollado los tratados internacionales aprobados en diciembre de 1996, sobre derechos de autor, e interpretación y ejecución de fonogramas, así como los trabajos en elaboración para la protección jurídica de las inversiones realizadas en bases de datos.

En este contexto se aprobó la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre Protección Jurídica de las Bases de Datos, que considera éstas como objetos susceptibles de protección de los derechos de autor. En cuanto a lo que se refiere a la selección o disposición de su contenido constituyen una labor de creación intelectual propia del concepto de autor, siempre que sea una base de datos original, y esto sin perjuicio de la libertad de los autores de esos contenidos de decidir si permiten, y de qué manera, la inclusión de sus obras en estas bases y sin menoscabo de los derechos existentes sobre su contenido.

Además de proteger los derechos de autor respecto a la originalidad de la selección y el contenido de la base de datos, se pretende proteger al fabricante contra la apropiación de los resultados obtenidos por las inversiones económicas y de trabajo hechas por quien buscó y recopiló el contenido y se considera que el objeto del derecho es garantizar la protección de la inversión en la obtención,

verificación o presentación del contenido de una base de datos, lo que implica el derecho a impedir la extracción o reutilización total o parcial no autorizadas

En nuestro actual código penal Ley No. 641 no están tipificados los llamados delitos informáticos. A lo que más se acerca esta norma legal es a la regulación de los derechos de autor y derechos conexos, lo cual está contemplado en su capítulo nueve, es decir estamos en igual posición que muchos países del mundo que no cuentan con una norma que regule los delitos informáticos.

19 Mencionan Chavarría, A, R, Pereira Vega, J, A y Lenin Ernesto Dávila, L, E, que **Los Tipos de delitos informáticos reconocidos por Naciones Unidas,** son:

1. "Fraudes cometidos mediante manipulación de computadoras, dentro de los cuales se encuentran:

   1.1 Manipulación de los datos de entrada.

   1.2 La manipulación de programas.

   1.3 Manipulación de los datos de salida.

2. Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo.

3. Falsificaciones informáticas" (Chavarría, et al, s.f).

Es por esto que muchos países se han preocupado por la elaboración de una norma que regule los delitos informáticos. Aquí se menciona como ejemplo a Costa Rica, que si bien es cierto no creó una ley en sí donde se establezcan los delitos informáticos, a su Código Penal Ley No. 4573, se le agregaron ciertos artículos para reprimir y sancionar los delitos informáticos.

Venezuela es otro de los países que cuenta con un decreto con fuerza de ley, sobre mensajes de datos y firmas electrónicas, Ley especial contra delitos

informáticos. Asimismo hay muchos países que en nuestros días cuentan solamente con un anteproyecto de ley. México es uno de éstos con su proyecto de ley sobre delitos informáticos, el cual fue presentado en el año 2000. Aquí habría que completar nuestra legislación, ya que solamente contamos con un anteproyecto de ley especial de delitos informáticos presentado en Octubre del 2004.

CONCLUSIONES

Como conclusión del presente trabajo de investigación sobre la sociedad de la información, las entidades de certificación y la firma electrónica, es importante mencionar que en definitiva la sociedad de la información ha dado paso a la creación de nuevas expresiones, como lo que se ha desarrollado en nuestra investigación, lo cual ha marcado a nuestra sociedad en general.

Hubo que mencionar en el presente trabajo algunas manifestaciones de lo que hoy en día conocemos como sociedad de información, dentro de las cuales se encuentra el comercio electrónico, las firmas electrónicas, y el gobierno electrónico.

Cabe mencionar que en el caso del comercio electrónico, pese a que Nicaragua no posee una ley que regule dicha materia, ya en la actualidad cuenta con lo que es el gobierno electrónico, es el caso de todo el complejo judicial, donde los abogados ya disponen de un portal virtual por medio del cual pueden verificar el estado en que se encuentran sus causas judiciales.

En cuanto a las entidades de certificación y a la firma electrónica, son notorios los grandes obstáculos que se ha tenido que superar para llegar formar parte de la sociedad de información.

Se menciona esto porque desde un principio uno de los problemas fue, como lo mencionamos en este documento, de que no habían razonamientos aceptables en cuanto al concepto de lo que es firma electrónica, hasta que se llegó a la conclusión de que sería lo que se conoce como firma electrónica avanzada y que en la mayoría de las actuales legislaciones sobre firma electrónica se introduce como firma electrónica reconocida.

Hoy en día estas entidades tienen mucho valor en nuestra sociedad, debido a que evitan los trámites que se hacen por documentos y se ahorra además, las grandes filas que se hacen para realizar una determinada gestión.

En cuanto a la regulación de las entidades de certificación, comercio electrónico y la firma electrónica, hay un gran desequilibrio entre todos los países del mundo, y por supuesto a nivel de América Latina.

Existen países muy avanzados en esto de las regulaciones y otros, como es de esperar con retraso. Así se vio que Colombia fue el primer país de América Latina en contar con una Legislación sobre Comercio Electrónico. Con posterioridad, se mencionó también a Panamá, Argentina, Chile, Uruguay Costa Rica, los cuales promulgaron leyes sobre mensajes de datos, firmas y certificados digitales.

Si bien es cierto que en nuestro país no se cuenta con la presencia de leyes que disciplinen la enorme masa existente de relaciones realizados por medios electrónicos, el Consejo Nicaragüense de Ciencia y Tecnología (CONICYT) puso un enorme grano de arena para abrir el camino hacia la inserción de la sociedad de la información con la realización del anteproyecto de ley de firma electrónica.

Con la regulación de esta nueva metodología, lo que se pretende es regular el uso y los efectos de la firma electrónica en los actos o contratos celebrados entre personas naturales o jurídicas llevados a cabo por la vía electrónica.

No obstante de que fue el CONICYT quien realizo la iniciativa de ley a la cual se hace referencia, al momento de llegar a la asamblea para su discusión ésta fue modificada, no en su totalidad, sino en artículos específicos, como en el que se establecía la denominación del ente regulador de las entidades de certificación. En el documento inicial se había propuesto a la Dirección de Acreditación de Firma Electrónica (DAFE). Actualmente, con la aprobación de la parte general de dicho proyecto, el aparato organizador será la Dirección General de Tecnología, (DGTEC), la cual depende del Ministerio de Hacienda y Crédito Público, dejando así al CONICYT sin ninguna atribución sobre la autorización de dichas entidades.

El presente trabajo llevó a un análisis sobre la seguridad jurídica que proporcionan los contratos electrónicos, los cuales tienen su nacimiento en el seno del comercio electrónico. Gracias a esto se ha tomado conciencia de que los contratos

electrónicos sí proporcionan seguridad jurídica a todas las transacciones realizadas en la red, tomando en cuenta la ley modelo de la CNUDMI y otras legislaciones que lo contemplan, tales como la Colombiana que en algunas ocasiones hace una copia fiel de las estipulaciones de la ley modelo, como lo mencionamos en el presente documento en cuanto a lo estipulado sobre el acuse de recibo, lo cual es una de las formas de proporcionar seguridad jurídica en las relaciones comerciales.

En cuanto al principio de equivalencia, se concluye que este es un balance que se otorga a los documentos electrónicos, para evitar discriminación alguna sobre éstos, por el hecho de realizarse a través de la red.

No debe haber la menor duda de que las firmas electrónicas cuentan con un gran valor probatorio, independientemente de no realizarse tradicionalmente como se ha venido haciendo desde décadas anteriores, es decir mediante el papel. Es así que estas pueden ser estipuladas como pruebas en juicios, siempre y cuando estén avaladas por una entidad de certificación, que dé certeza de su existencia y cumplan con los requisitos establecidos por la ley.

En cuanto a las entidades de certificación no hay más que decir que son las encargadas de emitir certificados electrónicos en relación a las firmas electrónicas. Debe dejarse en claro que en la ley modelo no se establece de manera expresa esta definición, pero sí se contempla lo que es un proveedor de servicios de certificación, al igual que en nuestro anteproyecto de ley sobre firma electrónicas, por su parte en la legislación de Panamá sí se encuentra conceptualizado lo que es una entidad de certificación.

Algo que se necesita señalar y que es significativo es lo relacionado a las auditorías, y es que éstas tienen que realizarse en todas las entidades de certificación para verificar su actuar, es decir que todo esté en regla bajo las leyes que las regule. Dichas auditorías de una o de otra forma se encuentran establecidas en la mayoría de las leyes que se nombran en el presente trabajo, empezando por mencionar la ley modelo de la CNUDMI.

También nos pareció de gran importancia el tema de los delitos informáticos, ya que hoy en día éstos son realizados a diario en la totalidad del mundo virtual. Es por esta razón que existen varios países que se han preocupado por la regulación de dichos actos ilícitos y han actuado de una u otra forma para lograrlo. Así Costa Rica, que si bien no creó una normativa sobre delitos informáticos, sí los incluyó en su código penal. Otra legislación es la venezolana, que también ha tomado cartas en el asunto.

Y para finalizar hay que decir que el anteproyecto de ley de firma electrónica de Nicaragua, está balanceado con respecto a las leyes de los demás países. Esto puede verse en la legislación de los países aludidos en el presente trabajo investigativo. Sin embargo, hay que ser razonables y mencionar también que en Nicaragua el problema no radica tanto en la falta de una ley, sino en la disponibilidad en nuestro país de la tecnología necesaria para llevar a cabo todos estos procesos vía electrónica. Pese a esto hay que ser positivos y continuar avanzando a partir de lo que ya tenemos.

RECOMENDACIONES

1. Es preciso que se aprueben los anteproyectos de ley que se encuentran en el seno de la Asamblea Nacional, el anteproyecto de ley de comercio electrónico y el anteproyecto de firma electrónica.

2. Realizar una reforma al Código de Procedimiento Civil para incorporar los documentos electrónicos como medios de prueba en el comercio electrónico.

3. Es necesario que las entidades de certificación actúen de manera imparcial al momento de emitir un certificado, para así brindar una labor completamente profesional y confiable.

4. Que las entidades de certificación cumplan con la realización de auditorías periódicamente para la verificación del buen funcionamiento de sus servicios.

BIBLIOGRAFIA

Autores

- Carreter, F. L. (2000) *Diccionario de datos*. España.
- Cubillos Velandia, R. y Rincón Cárdenas, E. *Introducción jurídica al comercio electrónico*.
- Davara Rodríguez, M. A. (1994). *Firma electrónica y autoridades de certificación: el notario electrónico. Cuaderno de derecho judicial No. 2. Consejo general del poder judicial.* España
- Mateu de Ros, R. (2004). *Consumidores y comercio electrónico.* Madrid, España.
- Orúe Cruz, J. R. (2003). *Análisis sobre el régimen jurídico de protección al consumidor en Nicaragua*.
- Talavera Silva, V. M. y Tórrez Zelaya, A. L. (2008). *La firma digital: Comercio Electrónico*. Tesis. Universidad Centroamericana. Managua, Nicaragua.
- Valdés, J. T. (2003). *Derecho Informático.*
- Vigil Gallo, S. A. y Vásquez Espinoza, D. A. (2009). Análisis crítico del Anteproyecto de Ley de Firma Electrónica presentado por el Conicyt a la luz del derecho comparado. Tesis. Universidad Centroamericana. Managua, Nicaragua.
- Wilson Pérez, M. H. (2009). *Sociedad de la Información para América Latina y el Caribe. Santiago de Chile*

Legislación

- *Anteproyecto de Ley de Comercio Electrónico de Nicaragua,* (2007).
- *Código Civil* . Nicaragua: Bitecsa.
- *Código Penal.* Nicaragua.
- *Ley General de Publicidad española*
- *Ley del Notariado*. Nicaragua
- *Ley 59, Ley de firma electrónica* (España, 2003).
- Ley modelo de la CNUDMI sobre firmas electrónicas con la guía para la incorporación al Derecho interno, (2001).
- Ley modelo de la CNUDMI sobre comercio electrónico, (1996).
- Ley No. 587, "Ley de Mercado de Capitales", (2006). Nicaragua.
- Ley 527: Del comercio electrónico y de las Firmas Digitales, (1999). Colombia.
- Ley 18.600, Documento electrónico y Firma electrónica, (2009). Uruguay

Sitios web

- Anónimo, (2008), *Economía de la Globalización,* consultada el 02 de Marzo del 2010 en http://www.iei.ua.es/dokuwiki/doku.php?id=sociedad_industrial
- Anónimo, (Marzo, 2010) *Fondo Monetario Internacional*. Consultado el 30 de Marzo del 2010 en http://www.imf.org/external/np/exr/facts/spa/groupss.htm
- Anónimo, (2010), *Firma Digital*. Consultado el día 28 de Abril del 2010 en http://es.wikipedia.org/wiki/Firma_digital.

- Anónimo, (2010). *e-gobierno.* Consultado el 28 de abril del 2010, de www.e-gobierno-Wikipedialaenciclopedialibre.mht

- Anónimo, (2010). *Comercio Electrónico*. Consultado el 06 de Julio del 2010 en http://www.culturaemedellin.gov.co/sites/CulturaE/SoyEmprendedor/Noticias/Documents/E-Commerce%20Universidad%20de%20Cuyo.pdf

- Burch, S. (2010), *Sociedad de la información/ Sociedad del conocimiento*, consultada el 03 de Marzo del 2010 en http://vecam.org/article518.html

- Contreras Díaz y Rivero Amador (2007), *Diseño del sistema de gestión de información del Centro de Estudios de Medio Ambiente y Recursos Naturales (CEMARNA) de la universidad de Pinar Del Río.* Consultado el 02 de Marzo del 2010 en http://www.gestiopolis.com/administracion-estrategia/sistemas-de-gestion-de-informacion-en-estudio-de-medio-ambiente.htm

- Castillo Jiménez, C, (2010) *La sociedad de la información y los derechos fundamentales. Ley 34/2002 de servicios de la sociedad de la información y del comercio electrónico,* consultado el 04 de Mayo del 2010 en http://www.uhu.es/derechoyconocimiento/DyC02/DYC002_A02.pdf

- Campiteni, y Rosso (2010). Consultado el 28 de Abril del 2010 en www.comercioelectronico-monografias_com.mht

- Cuervo, J. (2010). *Firma digital y entidades de certificación.* Consultado el 12 de Junio del 2010 en http://www.informatica-juridica.com/trabajos/firma_digital.asp

- Chavarría, Pereira Vega y Dávila. Corte Suprema de Justicia. (2005). Delitos Informáticos. Legislación y el Manejo de la Información en la era del Conocimiento. Managua, Nicaragua. Consultado el 18 de Junio del 2010 en http://www.ictparliament.org/resources/DelitosInformaticos.pdf

- Delarbre, R. T. (Septiembre-Diciembre 2001). La Sociedad de la Información . *Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación.* Consultada el 05 de Marzo del 2010 en http://www.terras.edu.ar/jornadas/30/biblio/30TREJO-DELARBRE-Raul-Revista-Iberoamericana.pdf

- Diaz bermejo, G. (2007). *La firma electrónica y los servicios de certificación, noticias jurídicas.* Consultado el 12 de Junio del 2010 en http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200712-123456789.html

- *Decreto 47, Ley para el reconocimiento de las comunicaciones y firmas electrónica, (2008).* Guatemala. Consultado el 08 de Junio del 2010 en http://www.congreso.gob.gt/archivos/decretos/2008/gtdcx47-2008.pdf

- Edutec. (Noviembre, 1997). *Revista Electrónica de Tecnología educativa, número 7* . consultada el 22 de Marzo, 2010 en http://www.uib.es/depart/gte/edutec-e/revelec7/revelec7.html

- Gil, J. M. (2004). Los observatorios de la Sociedad de la Información:Evaluación o política de promoción de las TIC en educación. *Revista Iberoamericana de Educación, No 36.* Consultada el 04 de Abril del 2010 en http://www.rieoei.org/rie36a02.pdf

- Gutiérrez, S. (2010). *Gestión de una Entidad de Certificación*. Consultado el 03 de Junio del 2010 en http://www.google.com.ni/search?hl=es&q=entidad+de+certificacion+de+samuel+gutierrez+T&aq=f&aqi=&aql=&oq=&gs_rfai=

- García Pérez, J. F. (2010). *Los derechos de autor en el entorno digital: entre el libre flujo y los usuarios*, consultado el 27 de Abril del 2010 en http://148.226.9.79:8080/dspace/bitstream/123456789/7361/1/Los%20derechos%20de%20autor.pdf

- González Echenique, L. (2010). *La firma electrónica: análisis del nuevo régimen jurídico contenido en la ley 597/2003, de 19 de diciembre.* Consultada el 17 de Junio del 2010 en http://www.revistasice.com/cmsrevistasICE/pdfs/ICE_813_153-171__53A03855324E882EF1F80C8790B5CDDD.pdf

- *La reforma a las Normas Financieras del Banco Central de Nicaragua, Resolución CD-BCN-14-3-09*, consultada el 28 de Abril del 2010 en www.asambleanacional.gob.ni/leyes/reformaalasnormasfinancierasdelbancocentraldenicaragua

- *Ley 34 del 11 de julio del 2002, de servicios de la sociedad de la información y de comercio electrónico*. España. Consultada el 04 de Mayo del 2010 en http://civil.udg.es/normacivil/estatal/contract/LSSI.htm consultada el 06/05

- *Ley No. 25326 Protección de los Datos Personales*, consultada el 04 de Mayo del 2010 en http://www.derhuman.jus.gov.ar/normativa/pdf/LEY_25326.pdf

- *Ley de Mediación y Arbitraje, Ley No. 540*. Nicaragua. Consultado el 28 de Abril del 2010 en www.asambleanacional.gob.ni/leyes/leydemediacionyarbitraje

- *Ley No. 43; Ley Que define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos*. Panamá. Consultado el 08 de Junio del 2010 en http://www.lexadin.nl/wlg/legis/nofr/oeur/arch/pan/ley43.pdf

- Ley No. 151, *Ley de Gobierno Electrónico, (2004). Puerto Rico.* Consultado el 08 de Junio del 2010 en http://www.ogp.gobierno.pr/PDF/Ley151.pdf

- *Ley de certificados, firmas digitales y documentos electrónicos en Costa Rica y entró a regir en el país el reglamento de la firma digital el 21 de Abril del*

2006. Consultada el 03 de Junio del 2010 en http://www.la-firma-digital-en-Costa-Rica.html

- López Pulido, J. P. (2010). *Marco jurídico de los servicios de la sociedad de la información y el conocimiento. El comercio electrónico. La firma electrónica*. Consultado el 17 de Junio del 2010 en http://www.hacienda.go.cr/centro/datos/Articulo/Sociedad%20de%20la%20informaci%C3%B3n%20y%20el%20conocimiento.pdf

- Muñoz Esquivel, O. (2001). Actividad De Las Entidades De Certificación Frente La Función Notarial. *Revista de derecho informático*. Consultado el 09 de Mayo del 2010 en http://www.alfa-redi.org/rdi-articulo.shtml?x=695

- Martín Reyes, M. A. (2001). Las entidades de certificación. *Revista de derecho informático.* Consultado el 09 de Mayo del 2010 en http://www.alfa-redi.org/rdi-articulo.shtml?x=703

- Márquez, J.A. (2007). Las Preguntas más comunes en la Contratación Electrónica. *Revista de Derecho Informático*. Consultado el 03 de Junio del 2010 en http://www.alfa-redi.org/rdi-articulo.shtml?x=8768

- Márquez, J.F. (2010). *Elementos de la contratación electrónica. El acuse de recibo y la confirmación del mensaje.* Consultado el 07 de Julio del 2010 en http://www.portaldelcomerciante.com/UserFiles/97/File/Ley%20Modelo%20sobre%20Comercio%20electronico.pdf

- Nieto Melgarejo, P. (2010). *El derecho de información en la contratación electrónica en base a la legislación española y europea.* Consultado el 07 de Julio del 2010 en http://www.elderechodelainformacionenlacontratacionelectronicaenbasealalegislacionespañolayeuropea.pdf

- Reyes Krafft, A. A. (2002). *La firma electrónica y las entidades de certificación.* Consultado el 03 de Junio del 2010 en

http://www.cervantesvirtual.com/servlet/SirveObras/01159852653479324108813/008469.pdf.

- Rodríguez, G. S. (Agosto, 2005), *Cumbre sobre la Sociedad de la Información: Desafíos*. Consultado el 05 de Marzo del 2010 en http://www2.bvs.org.ve/scielo.php?pid=S1315-62682005000200004&script=sci_arttext&tlng=es

- Reyes Ruiz, J. B. (2009). *Abordaje jurídico social del ejercicio de las entidades notariales de certificación y sus repercusiones en la fe pública del notario*. Tesis. Universidad de san Carlos de Guatemala. Consultado el 12 de Junio del 2010 en http://biblioteca.usac.edu.gt/tesis/04/04_7924.pdf

- Torres Torres, A. Y. (2009). *Principios fundamentales del comercio Electrónico y su desarrollo legislativo en Colombia y Latinoamérica.* Tesis. Universidad Carlos III de Madrid. España.

- Ortega, J (2009), *Apuntes sobre el Anteproyecto de Ley de Comercio Electrónico de Nicaragua*, consultado el día 28 de Abril del 2010 en www.apuntessobreelanteproyectodeleydecomercioelectronicodenicaraguajuanortega.mht

ANEXOS

INFORME DE CONSULTA Y DICTAMEN

Mangua 27 de Enero del 2010

Ingeniero
René Núñez Téllez
Presidente
Asamblea Nacional

Honorable Señor Presidente:

La Comisión de Justicia y Asuntos Jurídicos ha estudiado con detenimiento el Proyecto de Ley denominado Ley de Firma Electrónica, para su debida consulta y dictamen.

I. Consulta.-

1. Objeto de la Ley.-

El Objeto de esta Ley es regular el uso y los efectos de la firma electrónica en los actos y contratos celebrados entre personas naturales o jurídicas llevados a cabo por medios electrónicos.

2.- Consultas y modificaciones realizadas

En el proceso de consulta, se conto con la asesoría del Dr. Alfredo Chirino Sánchez, (asesor de nacionalidad Costarricense, experto en la materia) quien sirvió de relator en las consultas realizadas con la sociedad civil y expertos nacionales, en su informe ante la comisión manifestó que realizo una revisión al proyecto de ley constatando que el proyecto se encuentra dentro de los parámetros que exige la Ley Modelo de la UNCITRAL (Unificación del Derecho Mercantil Internacional) así como de la Ley Modelo de la OEA (Organización de Estados Americanos)

En este proceso se conto con los siguientes aportes personales e institucionales:

1. Asociación de Bancos de Nicaragua (ASOBAN)
2. Cámara de Comercio de Nicaragua
3. Ministerio de Hacienda y Crédito Público
4. CONICYT
5. Pro Cafta de USAID
6. Expertos Académicos Nacionales
7. Ministerio de Fomento Industria y Comercio

Todos los aportes proporcionados a la comisión, fueron recogidos al momento de la redacción del texto de ley, en virtud que mantenía el objeto con que fue concebida la iniciativa por los proyectistas.

Entre los temas debatidos se encuentran el establecimiento de requisitos para ser proveedor de servicios de certificación, requisitos que la iniciativa carecía, se puede destacar la contratación que se tendrá que hacer por los proveedores de Notarios Públicos, con cinco años de experiencia profesional, a fin de que puedan dar fe pública sobre el cumplimiento de las obligaciones del proveedor de servicios en el momento del libramiento del certificado al titular.

Se destaca también la designación a la Dirección General de Tecnología, dependencia del Ministerio de Hacienda y Crédito Publico, como en ente rector del proceso de acreditación de firma electrónica

4. Consideraciones hechas por la Comisión.

Las razones y justificaciones que nos han impulsado a proponer los cambios a esta iniciativa de ley son las siguientes:

1. Nicaragua avanza aceleradamente hacia la actualización en materia de tecnologías de información y de las comunicaciones. En los últimos años esta evolución tecnológica ha revolucionado a nivel mundial las diferentes áreas del conocimiento y de las actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicarse y celebrar negocios, al mismo tiempo ha contribuido a traspasar fronteras, disminuir el tiempo y acortar las distancias.

2. El objetivo en general es regular el uso de la firma digital, otorgándole validez y eficacia jurídica. Lo que busca es optimizar la actividad de la administración pública por medio de la sustitución del papel por el uso de medios electrónicos.

3. Así como también fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las administraciones públicas. De este modo, se incrementa el crecimiento y la competitividad de la economía y el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet.

4. La particularidad de estas tecnologías de información es que utilizan medios electrónicos y las redes nacionales e internacionales adecuadas para ello, que constituyen una herramienta ideal para realizar intercambios de todo tipo incluyendo el comercial a través de las transferencia de informaciones de un computador a otro sin necesidad de la utilización de documentos escritos en papel, lo que permite ahorros de tiempo y dinero.

5. El derecho debe estar presente en estas actividades con el fin de proteger a través de sus normas los intereses de los usuarios. En consecuencia, se hace necesaria e inminente la regulación de las modalidades básicas de intercambio de información por medios electrónicos, de las cuales han de desarrollarse todas las nuevas modalidades de transmisión y recepción de información, conocidas y por conocerse, con el fin de garantizar un marco jurídico mínimo indispensable que permita a los diversos sectores involucrados desarrollarse y contribuir con el desarrollo de las nuevas tecnologías.

6. La firma electrónica podrá ser utilizada en múltiples aplicaciones en especial en procesos automatizados, como la realización de pedidos a la omisión de facturas, esto permitirá minimizar transacciones comerciales.

7. La importancia de esta ley emanan de una realidad consistente en el hecho de que los medios de comunicación modernos tales como el correo electrónico, se han difundido su uso con gran rapidez en las operaciones comerciales tanto nacionales como internacionales lo que hace presumir que este tipo de comunicación es y será preponderante en el presente y en el futuro.

8. La actividad comercial es vital para el desarrollo económico de Nicaragua y es necesaria la correcta actualización de la legislación sobre esta materia. Por este motivo, los usuarios que dispongan de firma electrónica pueden consultar datos de carácter personal, realizar trámites u otras gestiones o acceder a diferentes servicios. La firma electrónica es un elemento de primera necesidad, que permite la firma de contratos en la red, el envío de información confidencial segura, y la relación telemática con sus sedes en todo el mundo o dentro del propio país, sin la necesidad de ningún traslado físico.

9. La firma electrónica permite ahorrar tiempo y dinero en la gestión de documentos y simplifica los procedimientos y la calidad del servicio. Proporciona el máximo grado de confidencialidad y seguridad en Internet. Así como también identifica a las partes que se conectan telemáticamente. Las oportunidades que ofrecen la firma electrónica a las economías en desarrollo para acelerar las transformaciones económicas son numerosas y atendiendo a las circunstancias de nuestro país con la aprobación del CAFTA es vital importancia tener una ley que regule la firma electrónica.

10. Esta iniciativa de ley comprende XI capítulos, el primero relativo a las disposiciones generales, el segundo de los certificados de firma electrónica, el tercero el uso de la firma electrónica en el Estado, el cuarto de la entidad rectora el quinto de los proveedores de servicios de certificación, el sexto de la acreditación de los proveedores de servicios de certificación, el capitulo séptimo hace referencia a los derechos y obligaciones del titular de firma electrónica, el capitulo octavo a las infracciones y sanciones el capitulo noveno de los recurso el decimo acerca de las disposiciones transitorias y el onceavo de las disposiciones finales.

II. DICTAMEN

Por todas las razones de índole doctrinaria, legal y constitucionalmente expuestas en este informe y tomando en cuenta que el Proyecto de Ley es necesario, estando bien fundamentado y no se opone a la Constitución Política, Leyes Constitucionales ni Tratados ratificados por el Estado de Nicaragua. La Comisión de Justicia y Asuntos Jurídicos dictamina favorablemente el Proyecto de Ley de Firma Electrónica y pide la plenario apruebe el presente dictamen. Adjunto copia del texto del Proyecto de Ley dictaminado con las reformas incorporadas.

MIEMBROS DE LA COMISION DE JUSTICIA Y ASUNTOS JURIDICOS

DIP. JOSE BERNARD PALLAIS A. DIP. MARCELINO GARCIA QUIROZ.

DIP. LUIS ULISES ALFARO DIP. YASSER MARTINEZ

DIP. CESAR CASTELLANO M DIP. MAXIMINO RODRIGUEZ M.

DIP. MARIA LIDIA MEJIA DIP. NOEL PEREIRA MAJANO

DIP. EDWIN CASTRO RIVERA DIP. ADOLFO MARTINEZ COLE

DIP. ALEJANDRO RUIZ JIRON N. DIP. RAMON GONZALEZ

LEY N0._____

LA ASAMBLEA NACIONAL DE LA REPÚBLICA DE NICARAGUA

CONSIDERANDO

I

Que esta convergencia tecnológica ha revolucionando la forma en que la sociedad produce, guarda y utiliza la información.

II

Que las nuevas tecnologías están trasformando las prácticas tradicionales de comercio al permitir la interconexión directa de los sistemas críticos de comercio y sus componentes claves, clientes proveedores, distribuidores y empelados que posibilitan el comercio y mercados globales.

III

Que todas estas disposiciones señaladas en este proyecto de ley, encuentran asidero en los estándares internacionales existentes en materia de protección comercio electrónico y firma electrónica, y en un marco doctrinal y explicativo que ya cuenta con gran solidez en el marco latinoamericano.

IV

Que el presente proyecto de ley resulta indispensable para complementar los derechos que establece la Constitución Política.

V

Que la legislación civil y comercial de la República de Nicaragua rigen cuestiones entre los particulares y empresarios atraves de contratos con efectos civiles, mercantiles y por ende son el fundamento esencial del comercio electrónico entre particulares.

VI

Que se necesita mantener la competitividad del país en actividades comerciales donde la tutela de los datos personales es preocupación central.

Ley No._____

El PRESIDENTE DE LA REPUBLICA DE NICARAGUA

Hace saber al pueblo nicaragüense que:

La Asamblea Nacional de la República de Nicaragua

En uso de sus facultades,

HA DICTADO

La siguiente:

LEY DE FIRMA ELECTRONICA

CAPITULO I
Disposiciones generales

Artículo 1.- Objeto de la Ley
La presente Ley tiene por objeto regular el uso y los efectos de la firma electrónica en los actos o contratos celebrados entre personas naturales o jurídicas llevados a cabo por medios electrónicos.

Artículo 2.- Ámbito de aplicación
Las disposiciones de la presente ley serán aplicadas dentro del territorio nacional a todos los actos o contratos en que se utilice firma electrónica en el contexto de las actividades no comerciales y comerciales, que garanticen su autenticidad e integridad de los documentos electrónicos.

Artículo 3.- Definiciones
Para los fines de la presente ley se entiende por:
a) Acreditación voluntaria: Autorización que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y se dicta, a petición del proveedor al que se beneficie, por el organismo público encargado de su acreditación y supervisión;
b) Certificado: Es la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta;
c) Certificado de firma electrónica: Es el documento electrónico firmado electrónicamente cuyos datos son vinculados a su titular, y suministrado por un proveedor de servicios de certificación;
d) Certificado digital: Certificación electrónica que da fe sobre los datos que identifican a quien posee la llave pública suscrita en el certificado digital.
e) Certificador: La entidad proveedora de servicios de certificación de firma electrónica;
f) Clave criptográfica: En un criptosistema asimétrico es aquella que se utiliza para acceder a un

documento con firma electrónica.
g) Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar electrónicamente y su correspondiente clave pública para verificar dicha firma electrónica.
h) Datos de creación de firma: Son los datos únicos, códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica;
i) Dispositivos de creación de firma: Es un mecanismo que sirve para aplicar los datos de creación de firma;
j) Dispositivo seguro de creación de firma: Es el mecanismo de creación de firma que cumple los requisitos establecidos en la presente Ley y su reglamento;
k) Datos de verificación de firma: Son los datos, códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica;
l) Dispositivo de verificación de firma: Es un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de firma;
m) Documento electrónico: Toda información generada, transferida, comunicada o archivada, por medios electrónicos, ópticos u otros análogos.
n) Encriptar: Es el acto de utilizar una clave única antes de intercambiar información.
o) Firma electrónica: Son datos electrónicos integrados en un mensaje de datos o lógicamente asociados a otros datos electrónicos, que puedan ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de datos;
p) Firma electrónica certificada: Es la que permite identificar al titular y ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que vinculada al mismo y a los datos a los que se refiere, permite que sea detectable cualquier modificación ulterior a estos;
q) Mensaje de datos: Es la información generada, enviada, recibida o archivada 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;
r) Proveedor de servicios de certificación: Entidades que otorgan, registran, mantienen y publican los certificados de firma electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas que pueden prestar otros servicios relacionados con la firma electrónica;
s) Producto de firma electrónica certificada: El programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas;
t) Titular: Es la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona que representa.

Artículo 4.- Interpretación de la Ley
En la Interpretación de la presente ley se tendrá en cuenta los métodos aceptados por el derecho común, así como las recomendaciones de organismos multilaterales en la materia, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.

Artículo 5.- Requisitos de validez de la firma electrónica certificada
Una firma electrónica certificada es válida si cumple los siguientes requisitos:
a. Que los datos de creación de firma correspondan exclusivamente al titular;
b. Que el certificado reconocido en que se base, haya sido expedido por un proveedor de servicios de certificación acreditado, y
c. Cuando el dispositivo seguro de creación de firma provenga de un proveedor de servicios de certificación acreditado.

Artículo 6.- Efectos jurídicos de la firma electrónica

La firma electrónica certificada tendrá el mismo valor jurídico que la firma manuscrita. Será admisible como medio de prueba en el proceso judicial o administrativo, valorándose ésta, según los criterios de apreciación establecidos en las leyes de la materia.

Cuando la ley exija la firma manuscrita de una persona, ese requisito quedará cumplido con una firma electrónica certificada. Se exceptúan los casos siguientes:
a. actos jurídicos del derecho de familia;
b. actos personalísimos en general;
c. disposiciones por causa de muerte;
d. aquellos actos que deban ser realizados bajo las formalidades exigidas por la ley de la materia o por aquellos acuerdos entre las partes.

Artículo 7.- Extinción de la firma electrónica
La firma electrónica se extinguirá por las siguientes circunstancias:
a. A solicitud de su titular,
b. Fallecimiento o incapacidad definitiva de su titular,
c. Por cese de la actividad del proveedor de servicios de certificación, en el caso de la firma electrónica certificada,
d. Disolución o liquidación de la persona jurídica, titular de la firma, y
e. Por causa judicial que así lo declare.

La extinción de la firma electrónica no releva de las obligaciones contraídas en el ámbito civil, administrativo, comercial, laboral y penal.

CAPITULO II
De los certificados de firma electrónica

Artículo 8.- Requisitos de validez de los certificados de firma electrónica
Los certificados de firma electrónica deberán cumplir con los siguientes requisitos de validad mínimos:
a. Indicar que el certificado se expide como certificado electrónico;
b. Identificar al proveedor de servicios de certificación y el país en que se encuentra establecido;
c. Contener el nombre y los apellidos del titular o un seudónimo que conste como tal;
d. Designar un atributo específico del titular, en caso de que fuera significativo en función de la finalidad del certificado;
e. Contener los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del titular;
f. Estipular una indicación relativa al período de validez del certificado;
g. Contener el código identificativo del certificado;
h. Identificar la firma electrónica certificada del proveedor de servicios de certificación que expide el certificado;
i. Determinar los límites de uso del certificado;
j. Establecer los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede; y

La consignación en el certificado de cualquier otra información relativa al titular requerirá su consentimiento expreso, siempre y cuando no contravenga la presente ley.

Artículo 9. Mensajes de datos firmados digitalmente
Se entenderá que un mensaje de datos ha sido firmado digitalmente si el símbolo o la metodología adoptada por la parte cumplen con un procedimiento de autenticación o seguridad establecido por el

reglamento de la presente Ley. Cuando una firma electrónica haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Artículo 10. Periodo de vigencia del certificado de firma electrónica
El certificado de firma electrónica es válido dentro del periodo por el cual fue establecido. Los certificados de firma electrónica quedarán sin efecto por el uso indebido, alteración, sustracción al proveedor autorizado, y además, por el incumplimiento de los requisitos de validez establecidos en la presente ley.

Artículo 11.- Reconocimiento de certificados extranjeros
Todo certificado de firma electrónica expedido en el extranjero será reconocido por la instancia rectora de acreditación de firma electrónica, en los mismos términos y condiciones establecidos en la presente ley, su reglamento o convenios establecidos para tal fin.

El Reglamento a la presente ley establecerá el procedimiento de reconocimiento.

CAPITULO III
Uso de la firma electrónica en el Estado

Artículo 12.- Uso de la firma electrónica en el Estado
Se autoriza el uso de la firma electrónica certificada a las instituciones del Estado, entes desconcentrados, descentralizados y autónomos; para que emitan documentos electrónicos, celebren toda clase de contratos electrónicos en sus relaciones entre sí o con personas naturales o jurídicas.

Se exceptúan aquellos casos mediante el cual la ley exija la solemnidad que no pueda ser satisfecha por la presente ley.

Artículo 13.- Validez de los actos, contratos y documentos electrónicos
Los actos, contratos y documentos electrónicos de las instituciones y entes referidos en el artículo anterior, suscritos mediante firma electrónica certificada, serán válidos y producirán los mismos efectos que los expedidos por firma manuscrita.

Artículo 14.- Notificación electrónica
Se autoriza a las Instituciones del Estado a realizar la notificación electrónica a las personas naturales o jurídicas, que sean parte de un proceso judicial o administrativo, en el domicilio del correo electrónico que designen para tal efecto los interesados y bajo su consentimiento.

En el caso de las personas jurídicas, la notificación se hará a su representante legal, abogado, fiscal o procurador designado en las oficinas que estos tuvieren o domicilio del correo electrónico que señalaren. El reglamento a la presente ley establecerá el procedimiento.

CAPITULO IV
De la entidad rectora

Artículo 15.- Entidad rectora de acreditación de firma electrónica
Se designa a la Dirección General de Tecnología, conocida en adelante como DGTEC, dependencia del Ministerio de Hacienda y Crédito Público, como el ente rector del proceso de acreditación de firma electrónica.

La DGTEC, además las potestades establecidas en las leyes de la materia, tendrá las siguientes:

a. Autorizar, inspeccionar y evaluar a los proveedores de servicios de certificación,
b. Cancelar o suspender la autorización otorgada a los proveedores de servicios de certificación,
c. Administrar el registro de proveedores de servicios de certificación, que para tal efecto se conformara dentro de la DGTEC,
d. Gestionar, por medio de la Dirección General de Ingresos, los ingresos provenientes de las tasas y multas establecidas en la presente ley,
e. Administrar y ejecutar su presupuesto de conformidad con la ley de la materia.
f. Supervisar la prestación de los servicios que brinden los proveedores de servicios de certificación,
g. Aplicar las sanciones administrativas que correspondan,
h. Seleccionar y contratar al personal técnico administrativo para el desempeño de sus funciones de conformidad con la ley de la materia,
i. Solicitar la información a los proveedores de servicios de certificación,
j. Realizar auditorías técnicas a los proveedores de servicios de certificación,
k. Velar por el cumplimiento de la presente ley y su reglamento,

Artículo 16.- Confidencialidad
El personal de la DGTEC, está obligado a guardar la confidencialidad de la información y custodia de los documentos que le entreguen los proveedores de servicios de certificación acreditados.

El Reglamento a la presente Ley establecerá las condiciones de confidencialidad.

Artículo 17.- Presupuesto
Los ingresos que la DGTEC gestione por los servicios que brinde ante los proveedores acreditados de servicios de certificación o ante cualquier otra persona natural o Jurídica, donaciones y ayudas financieras nacionales e internacionales formarán parte del tesoro público de conformidad con la ley 550 Ley de Administración Financiera y Régimen Presupuestario.

Artículo 18.- Tasas
Se establecen las siguientes tasas por los servicios de la DGTEC:
a. Por la acreditación de la prestación de servicios de certificación por un término de cinco años, se cobrará una tasa de un mil dólares de los Estados Unidos de América o su equivalente en moneda nacional.
b. Por la renovación de la prestación de servicios de certificación, se cobrará una tasa de quinientos dólares de los Estados Unidos de América o su equivalente en moneda nacional.

Artículo 19.- Facultades del director
El Director General de la DGTEC tendrá las siguientes potestades, sin perjuicio de las ya establecidas en la Ley 290 de Organización, competencia y procedimientos del Poder Ejecutivo sus posteriores reformas y su reglamento:
a. Representar legalmente a la DGTEC;
b. Suscribir los acuerdos, resoluciones y documentos relacionados con la entidad en mención,
c. Firmar los contratos del personal a su cargo,

d. Elaborar el informe de trabajo en la fecha correspondiente,
e. Suscribir convenios e instrumentos de colaboración con organismos afines a la entidad públicos o privados, nacionales e internacionales,

CAPITULO V
De los proveedores de servicios de certificación

Artículo 20.- Requisitos para ser proveedor de servicios de certificación
Para ser proveedor de servicios de certificación se requiere:
a. Un establecimiento permanente situado en territorio nicaragüense donde resida de forma continua o habitual, así como de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.
b. Emplear personal que tenga los conocimientos especializados, la experiencia y las calificaciones necesarias correspondientes a los servicios prestados. En particular, el personal deberá poseer competencia en materia de gestión informática. Conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados. Tal personal deberá poner en práctica los procedimientos administrativos y de gestión adecuada y conformes a normas reconocidas internacionalmente;
c. Contar con sistemas y productos fiables que estén protegidos contra toda alteración a fin de garantizar la seguridad jurídica, técnica y criptográfica de los procedimientos con que trabajan; y la confidencialidad de la información.
d. Ser persona jurídica debidamente constituida e inscrita en el registro público mercantil.
e. Disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente ley, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, según valoración de la entidad rectora.
f. Contratar a uno o varios notarios públicos con cinco años de experiencia profesional, a fin de que puedan dar fe pública sobre el cumplimiento de las obligaciones del proveedor de servicios en el momento del libramiento del certificado al titular

Artículo 21.- Obligaciones de los proveedores de servicios de certificación
Los proveedores de servicios de certificación está obligados a:
a. Garantizar la utilización de un servicio expedito, seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;
b. Garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;
c. Comprobar, de conformidad con la legislación correspondiente, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;
d. Contratar un seguro apropiado para responder por los daños y perjuicios que ocasione ante el titular de la firma electrónica o ante terceros;
e. Registrar toda la información pertinente relativa a un certificado reconocido durante un periodo de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;
f. 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, ante notario público con cinco años de experiencia profesional. 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;
g. Utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

1) Sólo personas autorizadas puedan hacer anotaciones y modificaciones,
2) Pueda comprobarse la autenticidad de la información,
3) 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
4) El agente pueda detectar todos los cambios que pongan en entredicho los requisitos de seguridad mencionados.

Artículo 22.- Responsabilidades de los proveedores de servicios de certificación
Los proveedores de servicios de certificación, son responsables de:
a. Los daños y perjuicios que en el ejercicio de sus funciones ocasionen por la certificación u homologación de certificados de firma electrónica. En todo caso, deberán demostrar que actuaron con la debida diligencia, se exceptúan los daños ocasionados en el uso indebido o fraudulento de un certificado de firma electrónica.
En ningún caso la responsabilidad proveniente de una certificación efectuada por un proveedor de servicio acreditado vinculará la responsabilidad pecuniaria del Estado.
b. Tomar medidas de seguridad efectivas contra la falsificación de certificados de firma electrónica y garantizar la confidencialidad de la información y resguardo de los documentos durante el proceso de generación de datos de creación de firma.
c. No almacenar ni copiar los datos de creación de firma electrónica de la persona a la que el proveedor de servicios de certificación ha brindado servicios de gestión de claves.

Artículo 23.- Requisitos de los dispositivos seguros de creación de firma electrónica
Los dispositivos seguros de creación de firma electrónica tendrán los siguientes requisitos mínimos:
a. Que los datos utilizados para la generación de firma solo puedan producirse una vez en la práctica y se garanticen razonablemente su secreto;
b. Que exista la seguridad razonable de que los datos utilizados para la generación de firma no puedan ser hallados por deducción y que la firma este protegida contra la falsificación mediante la tecnología existente en la actualidad;
c. Que los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.
Los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma.

Artículo 24.- Requisitos para la verificación segura de firma.
Durante el proceso de verificación de firma, se requiere lo siguiente:
a. Que los datos utilizados para verificar la firma correspondan a los datos mostrados al verificador;
b. Que la firma se verifique de forma fiable y el resultado de esa verificación figure correctamente;
c. Que el verificador pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados;
d. Que se verifiquen, de forma fiable, la autenticidad y la validez del certificado exigido al verificarse la firma;
e. Que figuren correctamente el resultado de la verificación y la identidad del firmante;
f. Que conste claramente la utilización de un seudónimo; y
g. Que pueda detectarse cualquier cambio pertinente relativo a la seguridad.

Artículo 25.- Protección de los datos personales.
Los datos personales del titular de la firma electrónica se protegerán en la presente ley y su reglamento de la siguiente manera:
a. El tratamiento de los datos personales relacionados con los proveedores de servicios de certificación para el desarrollo de su actividad y el que realice el ente regulador que contiene la presente Ley, se sujeta a lo dispuesto en la ley de la materia.
b. Los proveedores de servicios de certificación que expidan certificados de firma electrónica a los titulares solamente pueden recabar los datos personales de los titulares de los mismos y con su consentimiento expreso, con la exclusiva finalidad de expedir y mantener el certificado. En caso que

haya expedido un certificado a un Titular, utilizando un seudónimo, deberán constatar su verdadera identidad y conservar la documentación que la acredite.

CAPITULO VI
De la acreditación de los proveedores de servicios de certificación

Artículo 26.- De la acreditación de los proveedores de servicios de certificación
La acreditación es el acto mediante el cual el proveedor de servicios de certificación es autorizado a funcionar como tal por la DGTEC, habiendo demostrado su capacidad técnica, infraestructura, recursos humanos y económicos, así como programas informáticos necesarios para otorgar los certificados en el plazo establecido en la presente ley y en su reglamento, permitiendo su inscripción en el registro que para tal efecto se constituya.

Artículo 27.-Procedimiento de acreditación de los proveedores de servicios de certificación
El procedimiento de acreditación se llevará a cabo por medio de solicitud ante la DGTEC, la que adjuntará los requisitos establecidos en la presente ley. La DGTEC, resolverá sobre dicha solicitud en un plazo de sesenta días hábiles a partir de la recepción de la solicitud del interesado. Si pasado el término establecido la DGTEC no se pronunciare, la solicitud se entenderá aceptada. En tal caso, el proceso de registro operará de mero derecho conforme a la solicitud con acuse de recibo en mano del interesado.

Otorgada la acreditación, el proveedor de servicios de certificación será inscrito en el Registro que se lleve para tal efecto por la DGTEC. El proveedor de servicios de certificación está obligado a informar a la DGTEC, en un plazo no mayor de tres días hábiles, de cualquier modificación de las condiciones que permitieron su acreditación.

Artículo 28.- Causas de cancelación de la autorización
La DGTEC, podrá cancelar la autorización del proveedor de servicios de certificación en el registro, por las siguientes causas:
a.- A solicitud del proveedor acreditado;
b.- Por pérdida de las condiciones que motivaron su acreditación;
c.- Incumplimiento de las obligaciones establecidas en la presente ley y su reglamento.

CAPITULO VII
Derechos y obligaciones del titular de firma electrónica

Artículo 29.- Derechos del titular de firma electrónica
El **t**itular de firma electrónica tendrá los siguientes derechos:
a. A ser informado por el proveedor de servicios de certificación de todo lo relacionado con la creación y verificación de firma electrónica, así como de la prestación del Servicio;
b. A la confidencialidad en la información proporcionada a los proveedores de servicios de certificación;
c. A ser informado de los costos, uso, limitación de uso, procedimientos de reclamos en los servicios de certificación;
d. No transferir sus datos a otro proveedor de servicios de certificación sin su consentimiento expreso;
e. Acceder al registro de proveedores acreditados que tendrá la DGTEC;
f. Ser indemnizado y reclamar el seguro comprometido cuando corresponda.

Artículo 30.- Obligaciones del titular de firma electrónica

El titular de firma electrónica, tendrá las siguientes obligaciones:
a. Brindar datos exactos y completos;
b. Cuidar de manera responsable el mecanismo de seguridad para el funcionamiento del sistema de certificación que les proporcione el certificador;
c. Actualizar sus datos o cancelarlos cuando estime conveniente.

CAPITULO VIII
Infracciones y sanciones

Artículo 31.-Infracciones
Las Infracciones contenidas en la presente ley y su reglamento, se clasifican en leves y graves:

Artículo 32.- Infracciones leves
Son infracciones leves:
a. La entrega incompleta de la información o fuera del término previsto solicitada por la entidad rectora,
b. Emitir el certificado de firma electrónica sin llenar los requisitos totales de los datos,
c. Omitir el registro de los certificados expedidos,
d. Omitir la revocación en forma o tiempo de un certificado cuando corresponda hacerlo,
e. Incumplir las normas dictadas por la entidad rectora,

Artículo 33.- Infracciones graves
Son infracciones graves:
a. La negligencia en la seguridad de los servicios de certificación,
b. No permitir la inspección u obstruir la realización de las mismas o auditorias técnicas por parte de la entidad rectora,
c. Reincidir en la comisión de infracciones que dieran lugar a la sanción de suspensión,
d. Expedir certificados falsos,
e. La comisión de delitos en la prestación de servicios.
f. Uso indebido del certificado de firma electrónica por omisiones cuya responsabilidad es del proveedor de Servicios de certificación.

Artículo 34.- Establecimiento de sanciones
Para el establecimiento de las sanciones, se tomará en cuenta lo siguiente:
a. La gravedad de las infracciones cometida, así como su reincidencia,
b. El daño causado o beneficio reportado al infractor,
c. El efecto social de la infracción.

Artículo 35.- Sanciones administrativas
La DGTEC, sin perjuicio de las responsabilidades civiles y penales que correspondan, impondrá a los proveedores de servicios de certificación, o a sus representantes legales, o administradores, las siguientes sanciones administrativas:
a. Amonestación escrita,
b. Multa de cien a diez mil dólares de los Estados Unidos de América o su equivalente en moneda nacional,
c. Suspensión temporal de hasta dos años de la autorización de funcionamiento,
d. Cancelación de la autorización para continuar operando como proveedora de servicios de certificación.

CAPITULO IX
De los recursos

Artículo 36.- De los recursos administrativos
Los recursos administrativos que se interpongan ante la DGTEC, se tramitarán conforme lo establece la Ley No. 290, Ley de Organización, Competencia y procedimientos del Poder Ejecutivo, sus posteriores reformas y su reglamento.

CAPITULO X
Disposiciones transitorias

Artículo 37.- Plazo para la implementación de la Ley
Se autoriza a las instituciones del Estado, entes desconcentrados, descentralizados y autónomos para que implementen la presente ley en un plazo de un año calendario contado a partir de la entrada en vigencia de la misma.

CAPITULO XI
Disposiciones finales

Artículo 38.- Reglamentación
La presente Ley será reglamentada de conformidad con lo previsto en el numeral 10 del artículo 150 de la Constitución Política de Nicaragua, después de su entrada en vigencia.

Artículo 39.- Vigencia
Esta Ley entrará en vigencia a partir de su Publicación en La Gaceta, Diario Oficial.

Dado en la ciudad de Managua, en la Sala de Sesiones de la Asamblea Nacional, a los días del mes de del dos mil .- Presidente de la Asamblea Nacional. Secretario de la Asamblea Nacional.-

TEXTO ADOPTADO POR LA COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL EN
SU 29º PERIODO DE SESIONES, 28 DE MAYO A 14 DE JUNIO DE
1996, NUEVA YORK.

LEY MODELO DE LA "CNUDMI" SOBRE COMERCIO ELECTRONICO

ARTICULO 1

La presente Ley será aplicable a todo mensaje de datos que se ajuste a la definición del párrafo 1 del artículo 2 y que se refiera al comercio internacional.

ARTICULO 2

Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos

Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra

Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje

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

El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea Como contractual

ARTICULO 3

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

ARTICULO 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 otra forma 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 6
Escrito
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.

ARTÍCULO 7
Firma

Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

Si ese método es tan fiable como sea apropiado a los fines para los que se generó o comunicó el mensaje de datos

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

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 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

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

ARTÍCULO 9
Admisibilidad y fuerza probatoria de los mensajes de datos

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:

Por la sola razón de que se trate de un mensaje de datos

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

ARTÍCULO 10
Conservación de los mensajes de datos

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:

Que la información que contengan sea accesible para su ulterior consulta

Que se conserve todo dato que permita determinar el origen y el destino del mensaje, de haber alguno, y la fecha y la hora en que fue enviado o recibido

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

ARTÍCULO 11
Formación y validez de los contratos

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

ARTÍCULO 12
Reconocimiento por las partes de los mensajes de datos

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

ARTÍCULO 13
Atribución de los mensajes de datos

Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador

Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje

Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin

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

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

ARTÍCULO 15

Tiempo y lugar del envío y la recepción de un mensaje de datos

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

Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar

ARTÍCULO 16

Actos relacionados con los contratos de transporte de mercancías

Sin perjuicio de lo dispuesto en la primera parte 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:

Indicación de las marcas, el número, la cantidad o el peso de las mercancías

Declaración de la índole o el valor de las mercancías

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

Adquisición o transferencia de derechos y obligaciones con arreglo al contrato

ARTÍCULO 17
Documentos de transporte

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 realice por escrito o mediante un documento que conste de papel, se cumplirá ese requisito cuando el acto se realice por medio de uno o más mensajes de datos

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