# UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES


**TEMA:**

"LA FIRMA ELECTRÓNICA, TECNOLOGÍA DEL SIGLO XXI EN LA LEGISLACIÓN SALVADOREÑA"

**PRESENTACIÓN DEL INFORME FINAL DE INVESTIGACIÓN**
**PARA OPTAR AL GRADO DE:**

LICENCIADO EN CIENCIAS JURÍDICAS

**PRESENTADO POR:**

BR. LOPEZ FLORES, SARBELIO ENRIQUE

**DOCENTE DIRECTOR DE SEMINARIO:**

DR. GILBERTO ROMÁN ZÚNIGA VELIS

OCTUBRE 2007

SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA

## AUTORIDADES DE LA UNIVERSIDAD DEL EL SALVADOR.

MÁSTER. RUFINO ANTONIO QUEZADA SÁNCHEZ
RECTOR

MÁSTER. MIGUEL ÁNGEL PÉREZ RAMOS
VICERRECTOR ACADÉMICO

MÁSTER. OSCAR NOÉ NAVARRETE ROMERO
VICE-RECTOR ADMINISTRATIVO

LICENCIADO. DOUGLAS VLADIMIR ALFARO CHÁVEZ
SECRETARIO GENERAL:

DOCTOR. RENÉ MADECAEL PERLA JIMÉNEZ
FISCAL GENERAL

OCTUBRE, 2007

SAN SALVADOR, EL SALVADOR CENTRO AMÉRICA.

# AUTORIDADES DE LA FACULTAD DE JURISPRUDENCIA

DOCTOR. JOSÉ HUMBERTO MORALES
DECANO

LICENCIADO. OSCAR MAURICIO DUARTE
VICE-DECANO

LICENCIADO. FRANCISCO ALBERTO GRANADOS HERNÁNDEZ
SECRETARIO

OCTUBRE, 2007

SAN SALVADOR, EL SALVADOR CENTRO AMÉRICA.

**DEPARTAMENTO DE CIENCIAS JURÍDICAS.**

LICENCIADA. BERTHA ALICIA HERNÁNDEZ ÁGUILA

COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACIÓN:

DOCTOR. GILBERTO ROMÁN ZÚNIGA VELIS

DOCENTE DIRECTOR

LICENCIADO. ERICK LÓPEZ

ASESOR METODOLÓGICO

OCTUBRE, 2007

SAN SALVADOR, EL SALVADOR CENTRO AMÉRICA.

# DEDICATORIA.

A DIOS TODO PODEROSO

A mi Señor y Salvador Jesucristo por que él da la sabiduría y de su boca proviene el conocimiento y la inteligencia, hasta aquí me ha ayudado, guiado y fortalecido, a quien debo todo lo que soy y todo lo que tengo.

A MI MADRE

A mi querida madre, Leslie Evelyn Flores Avolevam, quien es mi ejemplo en la vida por su amor, apoyo y esfuerzo para poderme superar

A MI HERMANA

A mi hermana Leslie Mariel López de Lazo, por apoyarme en mis estudios.

Br. López Flores, Sarbelio Enrique

**ÍNDICE**

## CAPITULO II

## CAPITULO III

## CAPITULO IV

## CAPITULO V

## INTRODUCCIÓN

El presente documento, constituye un Proyecto de Investigación, donde se plantean las especificaciones técnicas de la fase de planificación para la realización de un estudio sobre La Firma Electrónica, Tecnología del Siglo XXI en la Legislación Salvadoreña.

El Objetivo general de la Investigación que se pretende realizar es: Conocer el funcionamiento de la Firma electrónica, el Ente que garantiza la utilización de esta herramienta, la seguridad y confidencialidad que se brinda para las contrataciones y transacciones económicas que se realizan en el Internet, y las ventajas y desventajas de la utilización de esta herramienta tecnológica.

El propósito del autor es cumplir con un requisito académico del Seminario de graduación, para poder optar al grado de Licenciado en Ciencias Jurídicas de la Facultad de Jurisprudencia y Ciencias Sociales, de la Universidad de El Salvador.

En el presente documento se pretende establecer, que La firma Electrónica es una herramienta tecnológica que nos dota de seguridad y confidencialidad en las actividades que se producen en el curso de la interacción humana, desde el momento en que nos comunicamos, contratamos, realizamos transacciones económicas, etc. se realizan on-line (a través de la Internet), es decir sin la presencia física de las partes y frente a la utilización pervertida de las nuevas tecnologías (aparición de los denominados delitos informáticos), que atentan contra la información, como bien jurídico de naturaleza colectiva o macro-social.

# CAPITULO I

## 1.0 PLANTEAMIENTO, FORMULACIÓN Y DELIMITACIÓN DEL PROBLEMA DE INVESTIGACIÓN.

## 1.1 UBICACIÓN DEL PROBLEMA DE INVESTIGACIÓN EN SU CONTEXTO SOCIO-HISTÓRICO.

### 1.1.1 ORIGEN Y EVOLUCIÓN HISTÓRICA

El comercio, es una actividad antiquísima del ser humano, la cual ha venido evolucionado de muchas maneras. Pero su objeto siempre ha sido el mismo. Se define: el Comercio es "el proceso y los mecanismos utilizados, necesarios para colocar las mercancías, que son elaboradas en las unidades de producción, en los centros de consumo en donde se aprovisionan los consumidores, último eslabón de la cadena de comercialización. Es comunicación y trato".[1]

Según lo expuesto, a través de los años han aparecido diferentes formas o tipos de comercio. A principio de los años 20 en Los Estados Unidos, apareció la venta por catálogo, impulsado por las grandes tiendas de mayoreo. Este sistema de venta, revolucionario para la época, consiste en un catálogo con fotos ilustrativas de los productos a vender. Este permite tener mejor llegada a las personas, ya que no hay necesidad de tener que atraer a los clientes hasta los locales de venta. Esto posibilitó a las tiendas poder llegar a tener clientes en zonas rurales, que para la época en que se desarrolló dicha modalidad, existía una gran masa de personas afectadas al campo. Además, otro punto importante de esto, es que los potenciales compradores pueden escoger los productos en la tranquilidad de sus hogares, sin la asistencia o presión, según sea el caso, de un vendedor. La venta por catálogo tomó mayor impulso con la aparición de las tarjetas de crédito;

[1] "Comercio Electrónico", www.monografia.com/trabajo12/monografias.html.

además de determinar un tipo de relación de mayor anonimato entre el cliente y el vendedor.

A mediados de los 80, con la ayuda de la televisión, surgió una nueva forma de venta por catálogo, también llamada venta directa. De esta manera, los productos son mostrados con mayor realismo, y con la dinámica de que pueden ser exhibidos resaltando sus características. La venta directa es concretada mediante un teléfono y usualmente con pagos de tarjetas de crédito.

A principio de los años 70, aparecieron las primeras relaciones comerciales que utilizaban una computadora para transmitir datos. Este tipo de intercambio de información, sin ningún tipo de estándar, trajo aparejado mejoras de los procesos de fabricación en el ámbito privado, entre empresas de un mismo sector. Es por eso que se trataron de fijar estándares para realizar este intercambio, el cual era distinto con relación a cada industria. Un ejemplo conocido de esto es el caso del Supermercado mayorista Amigazo. A mediados de los años 1980 esta empresa desarrolló un sistema para procesar órdenes de pedido electrónicas, por el cual los clientes de esta empresa emitían ordenes de pedido desde sus empresas y esta era enviada en forma electrónica. Esta implementación trajo importantes beneficios a Amigazo, ya que se eliminaron gran parte de errores de entregas y se redujeron los tiempos de procesamiento de dichas ordenes. El beneficio fue suficiente como para que la empresa Amigazo, instale un equipo a sus clientes habituales.

Por otra parte, en el sector público el uso de estas tecnologías para el intercambio de datos, tuvo su origen en las actividades militares. A fines de los años 70 el Ministerio de Defensa de Estados Unidos, inició un programa de investigación destinado a desarrollar técnicas y tecnologías que permitiesen intercambiar de manera transparente paquetes de información entre diferentes redes de

computadoras, el proyecto encargado de diseñar esos protocolos de comunicación se llamo "Internetting project" (de este proyecto de investigación proviene el nombre del popular sistema de redes), del que surgieron el TCP/IP (Transmission Control Protocol)/(Internet Protocol) que fueron desarrollados conjuntamente por Vinton Cerf y Robert Kahn y son los que actualmente se emplean en Internet. A través de este proyecto se logró estandarizar las comunicaciones entre computadoras y en 1989 aparece un nuevo servicio, la WWW (World Wide Web, Telaraña Global), cuando un grupo de investigadores en Ginebra, Suiza, ideó un método a través del cual, empleando la tecnología de Internet enlazaban documentos científicos provenientes de diferentes computadoras, a los que podían integrarse recursos multimedia (texto, gráficos, música, entre otros). Lo más importante de la WWW es su alto nivel de accesibilidad, que se traduce en los escasos conocimientos de informática que exige de sus usuarios.

El desarrollo de estas tecnologías y de las telecomunicaciones ha hecho que los intercambios de datos crezcan a niveles extraordinarios, simplificándose cada vez más y creando nuevas formas de comercio pero este comercio necesita de seguridad.

### 1.1.2 ORIGEN DE LA FIRMA ELECTRÓNICA A NIVEL INTERNACIONAL

Una de las cosas que desaparece en el comercio electrónico, es la firma manuscrita que puede ser reemplazada utilizando la Firma Electrónica. Unja firma electrónica sirve a las partes para autenticar todos y cada uno de los mensajes que se intercambian en el negocio electrónico y esta ofrece seguridad, pues se base a en un sistema de Criptografía, cuyo objetivo básico es encontrar sistemas que permitan llegar determinada información considerada secreta, desde un lugar de origen a otro destino, de forma tan segura que, si el mensaje es interceptado, el atacante no puede reconocer el mensaje.[2]

[2] "Criptografía y Firma Digital", www.webpanto.com.

La criptografía debe de ser abordada junto al tema de firma electrónica para poder comprender todo lo referente a esta. Puede decirse que la Firma Electrónica apareció en 1976 con la llegada de la criptografías de clave publica o asimétrica, sin embargo es hasta hace pocos años, que el gobierno y empresas empezaron a usar tecnologías de la firma electrónica para proteger documentos confidenciales en la red de redes

Para septiembre de 1998, el presidente de Estados Unidos de América, Bill Clinton y el primer ministro Irlandés Betier Ahern, firmaron electrónicamente un documento de comercio electrónico intergubernamental. Este es registrado como el primer documento de este tipo a nivel mundial que utiliza la tecnología de la firma Electrónica.

A causa del desenvolvimiento de relaciones comerciales el mundo entero a través de los nuevos canales que proporciona las nuevas tecnologías, generan una serie de incertidumbres desde el punto de vista jurídico, las que derivan, en la aplicabilidad de los principios generales de la contratación a la novedosa a contratación electrónica, se genera además incertidumbre de los medios, a través de los cuales esta clase de comercio se desarrolla, planteando problemas de autenticación, integridad y confidencialidad en la comunicación.

Como consecuencia, muchos países alrededor del mundo han hecho esfuerzos encaminados a disminuir dicha incertidumbre jurídica que han creado legislaciónes atinentes al comercio electrónico, dando un trato especial al manejo y desarrollo de la firma electrónica.

### 1.1.3 ORIGEN DE LA FIRMA ELECTRÓNICA EN EL SALVADOR

El llamado comercio electrónico ha emergido como negocio imparable. Los catálogos de los primeros negocios de cadena y tiendas, están siendo

paulatinamente remplazados por páginas Web, mientras día a día, mies de miles de personas se están decidiendo a utilizar este medio.

Toda esta serie de cambios, en la actualidad, han venido a destacar una serie de riesgos derivados del intercambio de información mediante redes abiertas, siendo la mas importantes: que el autor y fuente del mensaje sea suplantado; que el mensaje sea alterado en forma accidental o de manera maliciosa durante la transmisión; que el emisor niegue haberlo transmitido o el destinatario haberlo recibido y, que el contenido del mensaje sea leído por persona no autorizada. A fin de solucionar alguno de estos problemas es hacia a donde apunta precisamente la función de la Firma Electrónica.

Es por ello que en El Salvador, la incorporación de la Firma Electrónica como instrumento dentro del comercio electrónico y como reemplazo de los mecanismos tradicionales que vinculan a sujetos en relación con acuerdos de naturaleza comercial, ha sido gracias al sector importador, el cuál con el fin de facilitar y agilizar su labor, ha hecho uso de la tecnología de avanzada en materia de comunicación.

En la Ley de Simplificación Aduanera, se implementa un sistema llamado tele despacho, el cual funciona haciendo uso del Internet, por medio de este sistema la declaraciones de mercancías, están firmadas electrónicamente y se envía a la Dirección General de Renta de Aduanas. Dicho sistema fue desarrollado por el ministerio de Hacienda junto con la Cámara de Comercio e Industria de El Salvador a través de la Dirección Estratégica de Comercio Electrónico conocida como “DIESCO”, siendo esta, la encargada de ejecutar la parte técnica y encargándose de autenticar que la persona remitente de la información sea realmente la que quien dice ser.

## 1.2 ANTECEDENTES DE LA INVESTIGACIÓN

**Tesis**

LA SEGURIDAD JURÍDICA QUE PROPORCIONA EL ESTADO AL UTILIZAR LA FIRMA DIGITAL COMO MEDIO DE EXPRESIÓN DEL CONSENTIMIENTO.

**Acreditación**: Trabajo de graduación apara optar al titulo de Licenciado en Ciencias Jurídicas.

**Presentación:** Noviembre de 2004

**Comentario:** su tema central es hablar de la Firma Digital que no es mas que otra manera de garantizar la contratación con seguridad y confidencialidad, la seguridad tecnológica que representa y la seguridad jurídica que los Estados brinda en cuanto al su normativa, esto hace especial referencia a la regulación del Comercio mismo por el Internet que los estados hacen, tratando de dar regulaciones para al utilización del Internet.

## 1.3 IDENTIFICACIÓN DE LA SITUACIÓN PROBLEMÁTICA

El mundo avanza de forma acelerada en todo cuando tiene que ver con el desarrollo de tecnologías de información y comunicaciones, surgiendo nuevas formas de trabajar, aprender, comunicarse y celebrar negocios; borrando fronteras y acortando distancias.

La aparición del Internet en el mundo moderno, conlleva el empleo de Medios Electrónicos como una herramienta más, que en alguna medida han sustituido las tradicionales formas de búsqueda e intercambio de información, así como también en las formas de realizar operaciones comerciales, como la de contratar.

Este tipo de Herramientas nos ayudan a comunicarnos, haciendo transferencias o transacciones electrónicas en sentido amplio, realizándose en el sector publico para la comunicación con la Administración o con el Sector Privado, en las relaciones empresariales y de consumidores, tanto en el ámbito nacional e

internacional; estas nuevas herramientas, nos acercan en cuestiones de segundos a cualquier país del mundo, nos permite la agilización de las comunicaciones con cualquier persona, y su costo es mucho mas bajo, hoy por hoy, es de vital importancia en la sociedad en que vivimos, en la que el uso de nuevas tecnologías relacionadas con la transmisión de datos, se hace cada vez más cotidiano; y en donde todo parece señalar, que los documentos de elaboración electrónica reemplazarán poco a poco, a los documentos tradicionales.

Ante el fenómeno de las Globalizaciones, el uso de los medios electrónicos, es parte del mismo, era de suponer que ya las conocidas formas de contratar iban a sufrir un cambio radical en su forma.

El Salvador no ha querido quedarse atrás frente al fenómeno de la globalización, ya que el uso de Internet se ha generado a todos los niveles de la sociedad.

Con el afán de que cada persona, que utiliza día con día y en mayor medida el Internet, sus beneficios se ven de la necesidad de dotar de seguridad a aquellas comunicaciones electrónicas entre los mismos particulares, creando nuevas figuras inicialmente de carácter técnico como la Firma Electrónica, para luego dar un paso al marco jurídico apropiado que permita su implementación en nuestro país de manera real, generando la confianza necesaria para servir en el que hacer diario dotado de los aspectos legales necesarios.

En El Salvador, la firma Electrónica data desde los inicios de 1999; sin embargo, presenta un marco restado, que únicamente incluye la parte de Aduanas; en la misma regulación se reconoce la necesidad de un nuevo marco legal que permita su empleo por cualquier persona natural o jurídica, en los diversos aspectos de la vida cotidiana.

Siendo la solución del problema, un desafió para la realización de las transacciones electrónicas, la de solventar el problema de desconfianza que en torno a este existe, desconfianza generada por los factores culturales, jurídicos e incluso sociales, que inducen a las personas para no contratar por estos medios, agravándose por la especialización de grupos de personas que se encargan de boicotear las redes con la finalidad de producir un daño económico y lograr popularidad, personas denominadas “HACKERS” (piratas informáticos); ante esta realidad, se buscan alternativas que cumplan con aportar una seguridad real, dentro de los cuales se destaca la FIRMA ELECTRÓNICA dando una mayor confianza a la utilización de los documentos lo cual solventarían el problema de los documentos electrónicos, a priori, ya que su falsificación resulta técnicamente más sencilla que en los documentos físicos. El documento electrónico por lo que contiene únicamente información, no ligada a ningún soporte ni acción física concreta, la información podría alterarse sin dejar huella física alguna.

Evidentemente, esto abre las puertas a muchos tipos de fraude: falsificación de mensajes y cartas. Modificación maliciosa de las condiciones de los contratos, o suplantación de personalidad, por citar sólo algunos.

La Firma electrónica puede utilizarse como elemento de apoyo. Lo que pretende la firma es, esencialmente lo siguiente:

- Acreditar la validez de un documento, de modo que no pueda ser alterado o sustituido por otro.
- Vincular un documento a una persona o entidad.

Además, los métodos de cifrado que utiliza la firma electrónica, garantizan que cualquier mínima alteración en el documento original, producirá una versión cifrada notablemente distinta, pues es imposible, a efectos prácticos, generar tal

versión cifrada sin disponer de la clave, que el firmante conserva en su poder y no comunica a nadie.

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

El método no es matemáticamente infalible. Por ejemplo, ¿cómo estar seguros de que la clave pública es la del firmante y nadie nos ha engañado? Los sujetos que hacen posible el empleo de la firma electrónica, son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

Los prestadores de servicios de certificación, están obligados a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Además, están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Adicionalmente, el establecer obligaciones a los prestadores de servicios de certificación, en función de si estos emiten certificados, determinar su régimen de responsabilidad, debiendo tener en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

El nuevo régimen, nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos, para quienes los ofrecen al público.

En cualquier caso, aunque en teoría es posible la suplantación, la fiabilidad del método es suficiente para su uso práctico: al fin y al cabo, la firma manuscrita tampoco está a salvo de falsificaciones.

## 1.4 FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

Por todo lo anterior se formula el problema de investigación de la manera siguiente:

¿Será la Firma Electrónica una herramienta tecnológica que nos brinda seguridad y confidencialidad en la comunicación, contrataciones y transacciones económicas, etc., que se realiza en el Internet?

## 1.5 DELIMITACION DEL TEMA

El presente apartado, busca señalar los límites de la investigación a realizar, para de esta manera, exponer con precisión los aspectos que se desarrollarán en la misma, así como señalar algunos que no serán tomados en cuenta.

Para elaborar la delimitación, se tomaron en cuenta cuatro parámetros, estos son: en cuanto al enfoque, en cuanto al contenido, en cuanto al espacio y en cuanto al tiempo.

### 1.5.1 EN CUANTO AL ENFOQUE:

Por ser la Firma electrónica, un tema que puede ser investigado desde diversos puntos de vista. El presente trabajo estará dirigido a la elaboración de un análisis desde el punto de vista jurídico, y no implica la no utilización y consecuente explicación, de términos ajenos a los aspectos jurídicos; pues, si todo régimen legal regula aspectos que se originan en la realidad misma y al observar el funcionamiento de la Firma Electrónica, nos encontramos ante un fenómeno con raíces informáticas y técnicas etc., resulta indispensable el conocimiento de términos de esa índole para la elaboración de un análisis mas acertado

### 1.5.2 EN CUANTO AL CONTENIDO:

Con el fin de delimitar el contenido del tema a investigar en forma mas precisa, es necesario dividir este tema en varios apartados: El Internet y el Comercio Electrónico, la Firma Electrónica como sistema de seguridad, Entidades de Certificación, la Firma Electrónica en el panorama Internacional y el uso de la Firma Electrónica en el Sistema Bancario

En base a los aspectos antes mencionados, se tratara de hacer un análisis jurídico, pues el marco legal que lo regula es escaso, razón por la cual se hará el mejor de los esfuerzos en el estudio.

### 1.5.3 EN CUANTO AL ESPACIO:

Existen un alto número de países, que hoy por hoy, hacen uso de la Firma Electrónica, de los cuales en todos ellos, se recogen los principios básicos y similitud en cuánto al régimen legal se refiere, dependiendo del o los país que se traten, lo cual hace su estudio resulte muy amplio.

Como consecuencia de lo anterior, la presente investigación estudiará únicamente el régimen legal que norma la Firma Electrónica de El Salvador. Lo que no significa que en el análisis a elaborar, no se haga referencia a alguna Ley o figuras

jurídica extranjera, que pueda haber servido en la creación de las nuestras, es decir, que si bien esporádicamente se toma en cuenta una legislación que no sea salvadoreña, será para mayor comprensión de esta última, sin que la investigación a realizar pretenda ser un estudio, ni de Derecho comparado, ni de otras legislaciones.

### 1.5.4 EN CUANTO AL TIEMPO:

Tomando en cuenta, lo interesante que resultaría un estudio de La Firma Electrónica que parte desde la creación de la misma, es necesario en la investigación a desarrollar, hacer una delimitación en cuanto al período que abarcará la misma.

Por lo antes dicho, el análisis a desarrollar tendrá como objeto el régimen jurídico que lo regula en el salvador a partir de los años 90, época en la cual, el país y la población misma decimos alto a la guerra y al estancamiento siendo desde ahí, que El Salvador comienza con el progreso, gracias a los acuerdos de paz hasta en la actualidad, tratando de mejorar la calidad de vida , la seguridad social, ejerciendo la nueva democracia e incluyéndose como posible candidato a ser parte de los mercados financieros, y ser una actor más, en la globalización .

## 2.0 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Sabemos que la Tecno-era o Era Digital ha producido un drástico cambio de paradigma científico y social, con terribles impactos en el rediseño de la producción cultural y la industria; debemos señalar que las consecuencias de este nuevo paradigma tecnológico, que afectan y modifican la estructura social y económica, permiten distinguir las llamadas Economía de información (la capacidad de generación y manipulación de infraestructuras de información son decisivas para el desarrollo y expansión de las empresas), la Economía de Red (descentralización de las grandes empresas y formación de redes o alianzas con

pequeñas y medianas empresas que funcionan como auxiliares de aquéllas) y la Economía global o Globalización a secas (donde, en realidad, todos las áreas se encuentran subordinadas a este fenómeno: trabajo, comunicaciones, mercados financieros, cultura, etc.).

Pensemos en señalar que esta Sociedad de la Información, impacta sobre el orden regulador de conductas, el Derecho, e impone el re-análisis de las legislaciones y dogmas vigentes, las que no parecen adaptarse con docilidad a los nuevos fenómenos. La informática nos rodea y es una realidad incuestionable y parece que también irreversible. Está en casi todos los aspectos de la vida del hombre. Desde los más triviales hasta los más sofisticados. Sin la informática, las sociedades actuales colapsarían.

La informática se presenta como una nueva forma de poder, que puede estar concentrado o difuminado en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal.

Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva forma de energía, si se quiere intelectual, de valor inconmensurable, que potencia y multiplica de manera insospechada, las posibilidades de desarrollo científico y social, erigiéndose en patrimonio universal de la humanidad.

A medida que la informática se incorpora a más aspectos de la vida cotidiana, muchos trámites que tradicionalmente se realizaban en papel pasan a efectuarse de manera electrónica. Esto representa una ventaja para el tratamiento de la información.

Sin embargo, la propia naturaleza física del papel y la escritura han sido utilizadas también con ciertos fines. La dificultad de alterar un medio físico de representación

de la información, sirve como medida de seguridad contra las falsificaciones. La firma manuscrita, por otra parte, puede asociarse a su autor con un alto grado de certeza y sirve, por tanto, para acreditar su consentimiento, conocimiento o autorización en relación con la información escrita. Lógicamente, esto resulta fundamental en todo tipo de acuerdos, transacciones comerciales, etc.

En este contexto, la firma Electrónica es justificable por que se presenta como un instrumento de seguridad y confidencialidad desde el momento en que nos comunicamos, contratamos, realizamos transacciones económicas, etc., que se realizan on-line (a través de la Internet), es decir sin la presencia física de las partes y frente a la utilización pervertida de las nuevas tecnologías (aparición de los denominados delitos informáticos), que atentan contra la información como bien jurídico.

Esto además se Justifica atendiendo a:

**Interés & Prioridad Nacional**

Debe declararse el uso y la implementación de la Firma Electrónica:

- De interés nacional para garantizar y mantener la competitividad y promover el desarrollo del país y la inserción de los ciudadanos a la sociedad de la información.

- De prioridad gubernamental como herramienta eficiente para la gestión gubernamental para reducir costos, garantizar la transparencia y brindar mejores servicios a la ciudadanía.

- De prioridad empresarial, para modernizar y agilizar eficientemente los procesos y servicios y poder competir en un mundo digital, informatizado y globalizado.

**Sociedad de la Información & Desarrollo**

- En un mundo globalizado, de rápidos avances que transforman la forma en que vivimos y competimos, es vital usar la tecnología de la información y la comunicación como herramienta para el desarrollo de la nación.

- La Firma Electrónica, garantiza el acceso de nuestros ciudadanos al mundo de oportunidades que se abre con la sociedad de la información y así poder progresar todos como nación en ella.

## 3.0 OBJETIVOS

### 3.1 OBJETIVO GENERAL

- Conocer el funcionamiento de la Firma electrónica, el Ente que garantiza la utilización de esta herramienta; la seguridad y confidencialidad que se brinda en las comunicaciones, las contrataciones, transacciones económicas, etc., que se realizan en el Internet; y las ventajas y desventajas de la utilización de esta herramienta tecnológica.

### 3.2 OBJETIVOS ESPECÍFICOS

- Comprender el funcionamiento de la Firma Electrónica.

- Determinar el Ente que garantiza la utilización de esta herramienta, así como las funciones y obligaciones que este tiene.

- Analizar el grado de seguridad y confidencialidad que se brinda en las comunicaciones, en las contrataciones y transacciones económicas que se realizan en el Internet.

- Establecer las ventajas y desventajas de utilizar la Firma Electrónica como herramienta tecnológica.

- Conocer las normas reguladoras, y las pautas surgidas de Directrices, leyes modelos internacionales que resulten aplicables a estas actividades; así como profundizar en su interpretación y aplicación práctica.

## 4.0 MARCO DE REFERENCIA

### 4.1 MARCO TEÓRICO CONCEPTUAL

Para Andrea Sarra, la firma electrónica es la que "Se realizada mediante la transformación de un registro electrónico utilizando criptosistemas asimétricos y función hash, de modo que la persona que tiene el mensaje de origen y la clave pública del signatario puede determinar si la transformación se efectuó por medio de la clave privada que se corresponde con la clave pública que él tiene, y si el mensaje original fue alterado desde que se hizo la transformación."[3]

Según Apol-Lonia Martínez Nadal, la firma electrónica es: "la que se crea por medio de un sistema de criptografía asimétrica o de clave pública basados en el uso de un par de claves asociadas: una clave privada, que se mantiene en secreto, y una clave pública, libremente accesible para cualquier persona." [4]

Ramiro Cubillos Velandia, define la firma electrónica como: "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y todo método relacionado con un mensaje de datos que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos." [5]

---

[3] Sarra Andrea viciana « comercio Electrónico y derecho » Editorial Astrea, edición 2001, buenos aires. Pág. 389.
[4] Martínez Nadal, Apol-Lonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación, Tercera Edición, Editorial Civitas, Madrid, España. 2001. Pág. 42
[5] Cubillos Velandia, Ramiro y otro, Introducción Jurídica del Comercio Electrónico, Ediciones Jurídicas Gustavo Ibáñez, Bogotá, Colombia. 2002. Pág.215

También podemos encontrar definiciones de firma electrónica en Internet, tales como:

- "La firma electrónica está formada por una serie de caracteres de lo mas variado –letras, números, signos, etc.- elaborados con un programa informático, los cuales, al asociarse a otros datos, también de tipo electrónico permite entre otras cosas, identificar al firmante de los mismos." [6]

- "La firma electrónica es una cadena de caracteres, generado mediante un algoritmo matemático que se obtiene utilizando como variables la clave privada y la huella digital del texto a firmar, de forma que permite asegurar la identidad del firmante y la integridad del mensaje" [7]

- "La firma electrónica puede ser definida como una secuencia de datos que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo de cifrado asimétrico o de clave pública, y que equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje." [8]

- "La firma electrónica es un conjunto de caracteres que se añaden al mensaje que enviamos a través de Internet, con el objeto de proteger la integridad de los datos que se trasmiten, evitando que sean interceptados y falsificados. A través de esta codificación, el receptor del mensaje puede comprobar no solo el origen de los datos que se han remitido, sino su integridad y la identidad de la persona que los envió." [9]

[6] www.tuguialegal.com/firma digital/1.htm
[7] www.iec.csic.es/criptonomicon/seguridad
[8] www.espanol.groups.yahoo.com/groups/
[9] www.html.net/seguridad/varios/firma-certificado

## 4.2 MARCO NORMATIVO - LEGAL

### 4.2.1 FUNDAMENTO CONSTITUCIONAL

Que de conformidad a lo establecido en el Art. 53 de la Constitución de la República, es obligación del Estado el propiciar la investigación y el quehacer científico tendientes al logro de un desarrollo social y económico del país.[10]

Que la ciencia y la tecnología, son reconocidas como pilares fundamentales de la cultura de un país, que intervienen en el desarrollo económico y social, como factores determinantes para lograr una mejor calidad de vida y bienestar de la sociedad salvadoreña.

### 4.2.2 FUNDAMENTO LEGAL

#### 4.2.2.1"TLC"

Que el fomento de la incorporación del progreso técnico en los sectores productivos, dentro de un marco de creciente valorización de los recursos humanos, es un área en donde la participación del Estado es de fundamental importancia, como agente impulsador del proceso de innovación y de inserción en la economía internacional.

En El Salvador, se ha carecido de instituciones jurídicas de carácter tecnológico, en mención especial a la Firma electrónica y las entidades de Certificación no gozan de una regulación que cumpla con dar respuesta a la problemática que se suscita en la realidad, pues el marco regulatorio que existe y que hace referencia es el Tratado de Libre Comercio, entre Centroamérica, Republica Dominicana y los Estados unidos de América, denominada por sus siglas en español: TLC.

[10] Constitución de la Republica de El Savador (D.L. 38 de 15 de diciembre de 1983, publicada D.O. de 16 de diciembre de 1983.)

Teniendo este, la categoría de Ley Segundaria por el reconocimiento que se le da a nivel constitucional en el articulo 144 cn, en base a este articulo, se hace el reconocimiento de la aceptación del “TLC”, en nuestro caso en especial, del capitulo Catorce, respecto al Comercio Electrónico, poniendo a disposición lo necesario para concretar todos los aspectos importantes del comercio electrónico y en especial de la Firma Electrónica y las Entidades de Certificación.

En El salvador, el ministerio de economía, esta siendo el responsable de un documento (en su calidad de borrador) el cual en su oportunidad, pretende responder al compromiso internacional contraído en el “TLC” sobre el comercio electrónico, y, en especial, a la Firma Electrónica y las Entidades de Certificación

#### 4.2.2.2 “DECRETO 529”

En la Ley de Simplificación Aduanera (L.S.A)[11] , el objeto de es el plasmado en los considerándos de la misma al señalar la necesidad de adecuar los servicios aduaneros a los estándares de calidad y eficiencia en términos de facilitación del comercio internacional.

Encontramos pequeños rasgos, de lo necesario que se esta volviendo el uso de las nuevas tecnologías, en espacial de la Firma Electrónica y las Entidades de Certificación.

**Artículo 6.- (*)[12]**

La declaración para destinar aduaneramente las mercancías, deberá efectuarse mediante transmisión electrónica de la información, conforme los lineamientos y formatos físicos y electrónicos establecidos por la Dirección General, a través del sistema conocido como teledespacho, el cual, para asegurar la integridad de los flujos de información, deberá estar estructurado por procedimientos que aseguren

[11] Ley de Simplificación Aduanera (D.L. 529 de 13 de enero de 1999, publicada en el D.O. de 3 de febrero de 1999.)

[12] (*) El presente artículo ha sido reformado mediante D.L. No.523, D.O. N. 188, Tomo No.353, del 5 de octubre de 2001.

la autenticidad, confidencialidad, integridad y no repudiación de la información transmitida. Excepcionalmente, la declaración podrá efectuarse por otros medios legalmente autorizados o por disposiciones administrativas de carácter general dictadas por la Dirección General.

Para efectos de esta Ley, teledespacho constituye el conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten, dentro de un marco de mutuas responsabilidades, y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia Tributaria entre la Dirección General y los usuarios y auxiliares del servicio aduanero, bancos y en general, los operadores e instituciones controladoras del comercio exterior.

Los documentos contenidos en un soporte magnético, digital o electrónico producirá los mismos efectos jurídicos que los escritos en un soporte de papel; en consecuencia, lo dispuesto en el párrafo anterior, será aplicable a la declaración del valor en aduana y a cualquier otro documento en formato electrónico que conforme la legislación requiera adjuntarse a la declaración de mercancías. Cuando la Ley requiera que la información conste o que la misma sea presentada y conservada o archivada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, siempre que la información contenida en éste sea accesible para su ulterior consulta.

En todo trámite legal, no se dará aplicación a disposición alguna que sea óbice para la admisión como prueba de un mensaje de datos.

En esta ley, se habla de nuevas modalidades de tele despacho en el.

#### 4.2.2.2.1 CÓDIGO ADUANERO UNIFORME CENTROAMERICANO

Art. 75 y en el art. 8 párrafo tercero, también, pues el tele despacho constituye un conjunto de elementos tecnológicos de carácter informático y de comunicaciones, que pretende regular el conjunto de relaciones entre personas jurídicas o entes, que intervienen en el intercambio de información por vía electrónica.

En el art. 8 párrafo tercero, ya hay una definición de firma, **vinculación de una pareja de claves o llaves únicas y correspondientes entre si, una pública y otra privada, de manera tal que ambas se correspondan de manera exclusiva y excluyente, debiendo además la entidad certificadora, administrar un sistema de publicidad de las llaves públicas. La constituye la firma digital o electrónica**.

Además, con lo que respecta a las Entidades de Certificación, en el texto de la misma ley, se contempla desde su promulgación, la creación de estos entes, con el objeto de garantizar la autenticidad, confidencialidad, e integridad de información y que la autorización para poder operar, se la otorgará el Ministerio de Hacienda.

#### 4.2.2.3 "DECRETO 994"

En la Ley General Marítimo Portuaria[13], Título II. de lo Marítimo, Capítulo X., Régimen de Responsabilidad de los Armadores.
Artículo 90.- Intercambio Electrónico de Datos

Para la emisión de los documentos a que se refieren los Artículos anteriores, podrá emplearse cualquier medio por el que quede constancia de la información que contenga. Cuando el usuario y el armador o transportador hayan convenido

[13] Ley General Marítimo Portuaria (D.L. 994 de 19 de diciembre de 2002, publicada en el D.O. de 1 de octubre de 2002.)

en comunicarse electrónicamente, dichos documentos podrán ser sustituidos por un mensaje de intercambio electrónico de datos.

La firma podrá ser manuscrita, o bien estampada mediante facsímile o autenticada por un código electrónico.

Así también:

**Ley General Marítimo Portuaria, Título IV. de los Puertos, capítulo V, Régimen de Responsabilidad de los Operadores Portuarios**

**Artículo 206.- Intercambio Electrónico De Datos**

Para la emisión de los documentos a que se refieren los Artículos anteriores, podrá emplearse cualquier medio por el que quede constancia de la información que contenga. Cuando el usuario y el operador portuario hayan convenido en comunicarse electrónicamente, dichos documentos podrán ser sustituidos por un mensaje de intercambio electrónico de datos.

La firma podrá ser manuscrita, o bien estampada mediante facsímile o autenticada por un código electrónico.

#### 4.2.2.4 "DECRETO 742"

En la Ley de Anotaciones Electrónica en cuenta de Valores[14] en la parte de los considerados reconoce, legitima y justifica la necesidad: Que las bolsas de valores y las centrales de depósito y custodia de valores, para poder operar eficientemente y con seguridad, deben pasar del sistema tradicional de negociación de valores representados mediante papel, a formas de representación de valores por medios electrónicos. La firma podrá ser manuscrita o bien

[14] Ley de Anotación Electrónica de Valores en Cuenta (D.L. 742 de 21 de febrero 2002, publicada en el D.O. de 22 de marzo de 2002.)

estampada mediante facsímile autenticada por un código electrónico" así también en su articulado:

**Art. 1. Valores negociables.** Las anotaciones electrónicas en cuenta representan valores negociables mobiliarios, incorporados a un registro electrónico y no a un documento. Los valores desmaterializados o anotados, al igual que los títulos valores, son una especie de valor. En este apartado se nos define la naturaleza jurídica.

#### 4.2.2.5 DECRETO 697

En la Ley de Bancos[15] se tiene por objeto regular la función de Intermediación Financiera y las otras operaciones realizadas por los bancos, propiciando que estos brinden a la población un servicio transparente, confiable y ágil, que contribuya al desarrollo del país, es de esta manera que se da uso de las herramientas tecnológicas de la siguiente manera:

**Artículo 56.- Términos de Referencia Aplicables** (*)[16]

Para la elaboración de las normas a que se refiere el Artículo precedente, los bancos tomarán en cuenta:

**1)** Que los bancos podrán celebrar operaciones y prestar servicios con el público mediante el uso de equipos y sistemas automatizados, estableciendo en los contratos respectivos las bases para determinar las operaciones y servicios cuya prestación se pacte; los medios de identificación del usuario y las responsabilidades correspondientes a su uso; y los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

[15] Ley de Banco (D.L. 697 del 2 de septiembre de 1999, publicada en el D.O. de 30 de septiembre de 1999.)
[16] (*) El literal l) ha sido reformado mediante D.L. No. 955, D.O. No. 178, Tomo No. 356, del 25 de septiembre de 2002.

El uso de los medios de identificación que se establezca conforme a lo previsto en este literal, en sustitución de la firma autógrafa, producirá los mismos efectos que los que las leyes otorgan a los documentos correspondientes y en consecuencia, tendrán el mismo valor probatorio; cuando estas operaciones se realicen mediante contratos de adhesión, los modelos de dichos contratos deberán ser previamente depositados en la Superintendencia, quien podrá, mediante decisión fundamentada, en un plazo no mayor a treinta días a partir de la fecha del depósito del modelo, requerir los cambios necesarios, cuando contengan cláusulas que se opongan a la legislación o cuando se consideren violatorios a los derechos del cliente. En todo caso el Banco estará obligado a explicar al cliente las implicaciones del contrato, previo a su suscripción. (*)

**Artículo 60.- De los Sistemas de Pago y las transacciones electrónicas (*)[17]**

Las operaciones activas y pasivas que efectúen los bancos y otras instituciones a través de las cuentas que manejen en el Banco Central, podrán realizarse mediante intercambio electrónico de datos. Para tal efecto, tendrán validez probatoria los registros o bitácoras contenidas en los sistemas informáticos, las impresiones que reflejen las transacciones efectuadas por los mismos y los registros de firmas digitales o de números de identificación personal de los participantes autorizados en dichos sistemas. Las certificaciones extendidas, por el funcionario autorizado por el Banco Central para llevar registros y controles de lo anteriormente referido, tendrán fuerza ejecutiva contra la parte que incumplió. Las instrucciones que dicten los bancos al Banco Central, serán de carácter irrevocable.

Las operaciones a que se refiere el inciso anterior, pueden adoptar la forma de préstamos interbancarios, liquidación de operaciones resultantes de las cámaras

[17] (*) El presente artículo ha sido reformado mediante D.L. No. 955, D.O. No. 178, Tomo NO. 356, del 25 de septiembre de 2002.

de compensación, créditos y débitos directos, transferencias relacionadas con operaciones del Estado, transferencias desde y hacia el exterior y otras operaciones que realicen los bancos entre sí.

Los bancos deberán aceptar las instrucciones electrónicas para efectuar operaciones de débito o de crédito en las cuentas de sus clientes, que le sean enviadas por otros bancos. Cuando se trate de operaciones de débito éstas deberán ser ejecutadas de conformidad a lo previamente pactado entre su cliente y el originador.

### 4.3 ORGANISMOS INTERNACIONALES

**ONU**

La organización de las Naciones Unidas, por conducto de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMÍ, mejor conocida por sus siglas en inglés UNCITRAL), con sedes tanto en Nueva York como en Viena, se compone de 37 países. En la Ley Modelo sobre Firma Electrónica Articulo 2 literal a), se entenderá por tal: “los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos, e indicar que el firmante, aprueba la información recogida en el mensaje de datos”.

En la sesión del día 12 de diciembre de 2001, fue aprobada por el pleno de la 85 Sesión Plenaria de la Asamblea General, la Ley Modelo sobre las Firmas Electrónicas.

**UNCITRAL o CNIJDMI** Ley Modelo de Comercio Electrónico (dic. 1996) Conceptos Generales: firmas digitales, certificados digitales y entidades de certificación. Ley Modelo sobre Firmas Electrónicas (2001).

Actualmente, en UNCITRAL, se trabaja en un proyecto de Convención Internacional sobre Contratación Electrónica, que pretende conjuntar las dos Leyes Modelo (Comercio Electrónico y Firma Electrónica) en la que se pretende incluir algunos conceptos de privacidad de datos personales, protección al consumidor y nombres de dominio.

Existen muchas definiciones de Firma Electrónica, sin embargo consideramos que la mas completa es la establecida por la UNCITRAL: Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

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

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

Es aquél conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, contenido en un soporte magnético ya sea en un disquete, algún dispositivo externo o disco duro de una computadora y no de papel), que permite identificar a su autor, es decir que es el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

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

Después de lo anteriormente expuesto y según nuestra investigación, puedo concluir que la firma electrónica, es un conjunto de datos electrónicos que identifican a una persona en concreto, suele unirse al documento que se envía por medio telemático, como si de la firma tradicional se tratara, de esta forma el receptor del mensaje está seguro de quien ha sido el emisor; este mecanismo permite la confidencialidad y la seguridad de la información, tanto enviada como recibida por Internet.

## 5.0 SISTEMA DE HIPÓTESIS.

### 5.1 HIPÓTESIS GENERAL.

- A mayor grado de seguridad y confidencialidad que se brinde a través del Internet en actividades como: comunicación, contrataciones y transacciones económicas, etc., Mayor será la utilización de la Firma Electrónica como herramienta tecnológica.

**5.2 HIPÓTESIS ESPECÍFICAS.**

- ¿Brindará la Firma Electrónica la seguridad necesaria en actividades como: comunicación, contrataciones y transacciones económicas?

- ¿La firma Electrónica garantiza la Identidad de las personas que la utiliza como medio de comunicación a través de los medios electrónicos?

**6.0 MÉTODO Y TÉCNICAS E INSTRUMENTOS A UTILIZAR.**

Para realizar la investigación del tema: **"LA FIRMA ELECTRÓNICA, TECNOLOGÍA DEL SIGLO XXI EN LA LEGISLACIÓN SALVADOREÑA"**, utilizaremos la siguiente Metodología, en aplicación de los Métodos Generales: Análisis – Síntesis; Inducción – Deducción; y los Específicos: Bibliográfico – Documental.

En ese sentido, los métodos antes mencionados nos permitirían hacer guía conceptual útil a nivel teórico y práctico del análisis del problema: **"LA FIRMA ELECTRÓNICA, TECNOLOGÍA DEL SIGLO XXI EN LA LEGISLACIÓN SALVADOREÑA"** Pero además, de la investigación Bibliográfica – Documental, el estudio se ayudara de la utilización de otros métodos específicos de las Ciencias Sociales, tales como: Síntesis Documental, Síntesis Bibliográfica, Síntesis Hemerográfica.

**7.0 BOSQUEJO DE TRABAJO**

**INDICE**

**3.3** Clases de Firma

**3.3.1** La Firma Autógrafa

**3.3.2** La Firma Mecánica

**3.3.2.1** El Facsímile

**3.3.2.2** La Máquina de Firma

**3.4** Características de la Firma

**3.4.1** Identificativa

**3.4.2** Declarativa

**3.4.3** Probatoria

**3.5** Elementos de la Firma

**3.5.1** Elementos Formales

**3.5.1.1** Signo Personal

**3.5.1.2** El Animus Signando

**3.5.2** Elementos Funcionales

**3.5.2.1** Identificadora

**3.5.2.2** Autenticación

**3.6** Firma Electrónica

**3.6.1** Generalidades

**3.6.2** Concepto

**3.7** Encriptación o Cifrado de Datos

**3.7.1** Clases de Criptografía

**3.7.1.1** Cifrado de Llave Privada o Simétrica

**3.7.1.1.1** Características de las Llaves Privadas

**3.7.1.1.2** Desventajas del Cifrado Tradicional

**3.7.1.1.3** Funcionamiento de Claves Simétrica

**3.7.1.2** Cifrado de Llave Pública o Asimétrica

**3.7.1.2.1** Características Principales de las Llaves Públicas.

**3.7.1.2.2** Ventajas de la Criptografía Asimétricas

**3.7.1.2.3** Funcionamiento de Clave Asimétrica

**5.6.11** Barra Americana de Abogados (ABA) (American Association)

**5.6.11.1** Lineamientos de Firmas Digitales
(Digitales Signatura Guidelines)

**5.6.12** Global Business Dialog On Electronic Commerce (GBDE)

**5.6.12.1** El Sector Privado debe ser Líder

**5.6.12.2** Los Gobiernos deben evitar Restricciones Amplias al Comercio Electrónico

**5.6.12.3** Donde la Intervención Gubernamental es Requerida Debe ser para apoyar y reforzar un predecible, Consistente y Simple Ambiente Legal para el Comercio.

**5.6.12.4** Los Gobiernos deben Reconocer las Cualidades Únicas de Internet

**5.6.12.5** El Comercio Electrónico en Internet, Sería Facilitado en una base Internacional

**5.6.13** Recomendaciones Internacionales

**CAPITULO VI**

# CAPITULO II

## 2.0 EL INTERNET Y SU DESARROLLO

## 2.1 ORIGEN HISTÓRICO DEL INTERNET

El inicio de la historia de Internet, lo podemos situar en los años sesenta, con el establecimiento de los llamados “canales de paquetes autónomos de información”, los paquetes autónomos, son un método para fragmentar mensajes en sub partes llamadas precisamente “paquetes” y enviando dichos paquetes de información a su destinatario para que los reensamblara, lo cual permitía que varios usuarios al mismo tiempo pudieran compartir la misma conexión en pequeñas unidades que pueden enviarse separadamente.

Esta tecnología de los paquetes autónomos de información fue desarrollada en 1968 en los Estados Unidos, pero no fue sino hasta 1969, cuando fue utilizada por el Departamento de Defensa de los Estados Unidos, específicamente por la *Agencia para Proyectos de Investigación Avanzada*, la cual utilizó este sistema, como ya habíamos mencionado, con la finalidad de establecer un canal experimental diseñado como un medio de apoyo en la investigación militar, concretamente con el objetivo estratégico real, todavía sencillo, de asegurar el envío de la orden de abrir fuego desde un centro de control a las bases de misiles, aún después o más bien en el caso de que las Redes de comunicaciones hubieren quedado en parte destruidas por un ataque, con el cual, todas las bases quedarían en posibilidad de comunicarse entre ellas y con el centro control, para lo cual se aplica perfectamente el sistema de paquetes autónomos de información.[18]

Dicho canal, se denominó ARPAnet (Agencia para Proyectos de Investigación Avanzada), el cual utilizaba un Protocolo de Control de Canal (NCP) como su Protocolo de transmisión desde 1969 y hasta 1982.

[18]. Godwin, M., “La Ley de la Red: Problemas y Perspectivas”, Internet World, 1993, p. 47

El Plan inicial para el ARPAnet, fue distribuido en octubre de 1967 durante el Simposium en Principios Operativos de la Asociación de Maquinarias Computarizadas.[19]

El Primer Procesador de Información de Mensajes para el ARPAnet, fue instalado en la UCLA (Universidad de California, Los Ángeles) el primero de septiembre de 1969, el cual, únicamente contaba con 12 Kilobytes de memoria, era considerado una de las mejores computadoras de su tiempo. Sin embargo, se instalaron posteriormente otros adicionales en el Instituto de Investigaciones de Stanford (SRI), en la Universidad de California en Santa Bárbara (UCBS), y en la Universidad de Utah, respectivamente.

Se dice que Internet, que es conocido como el “canal de canales", tuvo su origen exacto en 1972, en octubre de ese año, tuvo lugar la Primera Conferencia Internacional sobre Comunicaciones Computarizadas, con sede en la Ciudad de Washington D.C., en ella, se realizó una demostración publica del ARPAnet.

Los representantes del proyecto alrededor del mundo, incluyendo Canadá, Francia, Japón, Noruega, Suecia, Gran Bretaña y los Estados Unidos, discutieron la necesidad de comenzar a trabajar en el establecimiento de acuerdos sobre protocolos, el InterNetwork Working Group (INWG) fue creado para comenzar las discusiones para llegar a un protocolo común, siendo nombrado como primer encargado Vinton Cerf, quien estuvo involucrado con el ARPAnet instalado en la UCLA(Universidad de California, Los Ángeles).

La propuesta para lograr una interconexión internacional de canales, lo cual era un asunto de canales independientes y autónomos interconectados por otros canales,

[19] R. Resnick y D. Taylor, “La Guía del Negocio de Internet: Montar la autopista de información para beneficiarse”, Editorial Sams, 1994, p. XXV.

tal y como los circuitos independientes de ARPAnet, era que estuvieran interconectados por procesadores de información de mensajes (IWs).

En el ARPANET, una de las ventajas sobre las cartas enviadas por correo, fue que en un mensaje de ARPAnet, una persona podía escribir despreocupada e impersonalmente a cualquier persona aún cuando fuera de mayor rango dentro del ejército, puesto que no se conocía ciertamente quien iba a recibir el mensaje y el receptor no se consideraba ofendido, ya que la despreocupación y la tolerancia de la informalidad eran naturales, porque el canal es más rápido, inclusive cuando dos usuarios en distintos lugares se comunicaban conectando sus computadoras y entablando una conversación alfanumérica; otra de las ventajas de ARPAnet que se consideraron, fue que a través de sus mensajes uno podía proceder inmediatamente al punto, sin necesidad de entablar conversaciones innecesarias, además de que los servicios de mensaje, dejaban constancia grabada de cada uno de los mensajes y que la persona que enviaba este y la que lo iba a recibir, no tenían que estar disponibles al mismo tiempo.

En el año de 1983, el ARPAnet, fue dividido en dos: ARPANET y MILNET, éste último fue integrado al Canal de Datos de la Defensa, creado en 1982 y ARPANET fue puesto fuera de servicio en el año de 1990.
El papel de ARPANET como canal pionero, fue sustituido por el NSFNET el cual con el tiempo sería suplido por el Canal Nacional de Investigación y Educación: **NREN**.
ARPANET, fue de suma importancia en el desarrollo de la Red, pues en su tiempo fue la más grande, rápida y más popular parte de la Red. Su estructura inicial fue influida por el hecho de que fue desarrollado para formar parte del control y comando central de la estructura de las fuerzas armadas de los Estados Unidos, durante el desarrollo de la Guerra Fría. Así, fue diseñado para sobrevivir a un

ataque nuclear, lo cual influyó en la descentralización que actualmente caracteriza a la Red.
Cuando ARPANET estaba en las primeras etapas de su evolución, otra tecnología estaba influyendo en el desarrollo de la Red: Los Canales de Ventas, que usaron la tecnología de los sistemas de correo electrónico y los extendieron a lo que nosotros llamarnos ahora "conferenciar" (chatear).

A finales de los setenta y principios de los ochenta, otro tipo de tecnología de canales comenzó a entrar al escenario, estos fueron los primeros canales de ventas y de investigación como BITNET y QWERUIOP879+.[20]

Como otros muchos aspectos de la comunicación por medio de computadoras, la conferencia interactiva es un concepto que influyó en la tecnología de las computadoras.

Desde 1945 hasta 1970 varios modelos para conferenciar cara a cara o vía correo regular se han desarrollado, un modelo que tuvo gran influencia es el denominado "Método Delphi".

El primer sistema Delphi en línea para conferenciar, fue iniciado en 1970 el primer hardware y software dedicado específicamente para conferenciar, fue el EMISARI, el cual fue implementado en 1971, de cualquier forma, los sistemas para conferenciar de computadora y de teletexto de los años setenta, tendieron a ser lentos y poco confiables y fueron primeramente aplicados en ambientes estructurados para tareas particulares.
Esto iba a cambiar a finales de los setenta y principios de los ochentas, con el surgimiento de canales económicos creados por los usuarios tales como USENET, BITNET Y FIDONET.

[20] IBIDEM, p. XXVII

El Protocolo de copia UNIX-TO-UNIX o UUCP, fue creado en 1976 y el cual tuvo gran éxito y fue adoptado por muchos canales por su gran facilidad para enviar y recibir correspondencia, para conferenciar y transferencia de archivos.

Otro sistema desarrollado fue THEORYNET, iniciado por Lawrence Landweber en la Universidad de Winsconsin en 1977, THEORYNET proporcionó facilidades de envío y recibo de correspondencia para más de 100 científicos e investigadores en computación. En mayo de 1979, Landweber tuvo un encuentro con representativos de ARPA, de la Fundación Nacional de Ciencia y científicos en computación de varias universidades, el propósito de dicho encuentro fue establecer la factibilidad de establecer un canal computarizado del Departamento de Investigación y Ciencia en Computación. Dicho encuentro sirvió para el eventual establecimiento del Canal de Investigación Científica en Computación (CSNET).

El CSNET fue establecido por dos razones, por una parte, el UUCP, los módems y el sistema de teléfono existente proveían un método disponible para la transferencia de datos, por otra parte, grandes facilidades computacionales fueron aumentando sobre todo a partir de que la Universidad de Wisconsin fue tomando mayor conciencia de las ventajas que la conexión de sistemas de cómputo de ARPANET le daba en la investigación y reclutamiento de estudiantes.

Una serie de propuestas del NSF fue generada y revisada. Los primeros diseños para el CSNET, fueron previéndolo como un Canal que se mantuviera por sí solo.

Durante 1980, el científico de ARPA Vinton Cerf, propuso un plan para una conexión de canales entre CSNET y ARPANET.

Este plan fue concebido por CSNET como un canal lógico compuesto de varios canales físicos. Las comunicaciones entre CSNFT y ARPANET serían arregladas para ser transparentes, esto es, los servicios en cada canal serian "accesados" a través de una serie de protocolos.

Una serie de protocolos de comunicación desarrollados por ARPA llamados TCP/IP serían usados para enviar la información entre los canales.

La conexión entre los canales podría ser a través de una conexión denominada Canal de valor agregado o VAN (Valué Added Network). La implementación de esta conexión entre canales y la importante decisión de hacer al TCP/IP disponible sin cargo, marcó la fundación de lo que posteriormente sería conocido como INTERNET.[21]

En agosto de 1980 durante la reunión de planeación de grupo de CSNET se adoptaron muchas metas: todos los investigadores deberían tener acceso a CSNET, y el costo por membresía debería graduarse de acuerdo al volumen y al nivel de servicio, CSNET debería ser eventualmente autosuficiente financieramente, y la implementación del proyecto debería costar menos de cinco millones de dólares y tomar menos de cinco años.

La primera fase del plan implementado por CSNET proveyendo acceso telefónico al e-mail, fue completada en junio de 1982, la segunda fase completada en 1983, incluía la implementación del primer servidor de nombres de dominio en la Universidad de Wisconsin. Este fue el principal impulsor del Servicio de Nombres de Dominio ahora utilizado ampliamente en los canales TCP/IP.[22]

[21] Clarke, R. A., "Un Marco regulador y normativo de las computadoras", La computadora y la ley de la información, vol. XIII, 1995 consultado en: www.findlaw.com

[22] Carroll, J. y Broadhead, R., "Manual Canadiense del Internet ", Editorial Prentice Hall, 1995, p 46

Este Servicio de Nombres de Dominio, dió facilidad al transporte de correspondencia en el cual la computadora de usuario a usuario no necesitó ya conocer el camino exacto al sitio del receptor. La información sobre envío de correspondencia puede ser generada por consulta a la base central de datos en el Servidor de Nombres de Dominio, para 1990 este sistema sustituyó al viejo método UNIX.

En el tiempo mencionado, otro canal haciendo uso de UUCP estaba listo y corriendo: USENET.

Un importante sistema para conferenciar (chatear) primeramente distribuido fue el Canal de Usuarios de Unix (Unix User Network o USENET) el cual implemento el UUCP o Unix to Unix Copy Protocol para transportar noticias. Se estima que actualmente hay más de diez millones de usuarios usándolo en computadoras que son parte de USENET.

USENET, es un ejemplo de una arquitectura cliente-servidor. Un usuario conecta una máquina la cual se conecta a otra máquina la cual ha adquirido la correspondencia de USENET de los pasados días, semanas u horas. Los usuarios miran los encabezados de la correspondencia en el grupo que les interesa, entonces el usuario envía un comando requiriendo el texto completo de una correspondencia particular o artículo, la máquina del cliente requiere el artículo particular para que le sea enviado por la máquina a la que se encuentra conectada la suya. Si el artículo no se encuentra disponible por cualquier razón, aparece un mensaje que indica: "artículo no disponible" y es transmitido al usuario, de otra forma; el texto completo del artículo requerido, deberá aparecer en la Terminal del usuario. El usuario entonces leerá el artículo o adquirirá el artículo, o una copia a través del correo electrónico.

USENET, se considera propiamente iniciado en 1979, como parte de una serie de proyectos escritos por el estudiante graduado de la Universidad de Carolina del Norte; Steve Bellovin, a fin de automatizar y facilitar la comunicación UUCP entre

dicha Universidad y la Universidad de Duke. Estos proyectos fueron reescritos y extendidos en un programa escrito en el lenguaje "C" de computadora por Steve Daniel y Tom Truscott, esta versión es generalmente conocida como la difusión de noticias "A".

Nuevos artículos son separados en divisiones llamadas grupos de noticias, cada división se supone limitada a un tema o tópico específico y el nombre del grupo debe dar una idea del contenido general del grupo. Estos grupos son organizados en jerarquías de tópicos relacionados.

El Canal de Noticias de USENET, comenzó con dos jerarquías: mod y net. La jerarquía mod contenía los grupos en que la persona es el moderador para editar y controlar la información. La jerarquía net contenía todos los demás grupos.

Posteriormente, Mark Glickinan y Mark Horton, escribieron la versión "B" de noticias, en 1981. Una serie de lanzamientos numerados del 2.1 al 2.10.2 aparecieron entre 1982 y 1984 los cuales fueron realizados primero por Horton y luego por Rick Adams del Centro de Estudios Sísmicos.

Entre 1986 y 1987, USENET sufrió una serie de constantes reajustes y reorganizaciones conocidas como el gran "Renombramiento". Desde su inicio USENET sólo tenía las jerarquías mod y net, esto fue pronto aumentado con la adición de los grupos "fa". Cuando una completa reorganización de USENET fue propuesta, comenzó una gran discusión y argumentación en línea.

La discusión se suscitó sobre todo con la creación de las siete jerarquías principales (comp, mise, news, rec, sel, soc, talk) y la supresión de los grupos mod, net y fa.

El gran renombramiento comenzó en julio de 1986 y terminó en marzo de 1987, y una de las razones de dicho renombramiento, fue el creciente número de grupos hechos como una reorganización de los dominios de mayor nivel.

Otra razón, fue el agregar grupos controversiales en el dominio talk los cuales fueron añadidos al final del renombramiento.[23]
El respaldo original del USENET, fue creado por Gene Spafford en 1983, en un intento de racionalizar la retransmisión de las noticias de USENET, sin embargo, fue sustituido debido al creciente número de tráfico de USENET que se estaba moviendo en las conexiones de ARPAnet, esto llevó al reemplazo de LJUCP por NNTP el cual es un método de transmitir las noticias de USENET con conexiones TCP/IP. Y muy pronto creció el número de sitios acompañados, por la creciente presión de democratización del proceso de creación de grupos de noticias.

Dos años después del inicio de USENET en Carolina del Norte, otro importante canal de ventas y desarrollo fue creado: BITNET (Because It's Time Network), que inició como un canal cooperativo en la Universidad de la Ciudad de Nueva York (CUNY).

El BITNET usa sistemas de correo electrónico y un mecanismo llamado “LISTSERV” para distribuir la información.

Una vez revisados los canales más importantes que se han desarrollado durante los últimos treinta años, cabe establecer que el ARPANET creó una Red en cadena que enlaza a los centros de cómputo más importantes, y al usar información dividida en paquetes autónomos, fue posible configurar una estructura flexible, independiente del tipo de computadoras utilizadas.

[23] En: www.cis.ohio-statc-edu/hvDertext/faa/usenet/coDvríght-FAQ/Dart2/faa.html

El uso de los protocolos TCP/IP que adoptaron con mucha rapidez el servicio militar en una Red independiente de MILNET y las universidades, se fortaleció en 1984, cuando la Fundación Nacional de Ciencias, (NSF) los seleccionó, al crear cinco importantes centros de Mando equipados con grandes computadoras, con el fin de permitir a toda la comunidad científica tener acceso a la información almacenada.

Entonces, cada centro universitario importante, estableció una conexión con la Red constituida por la NSF, la cual fungió como "soporte" o circuito principal para todo el tráfico de sub-Redes. De ahí en adelante, fue posible ingresar a cualquier punto en la Red, desde cualquier sitio universitario conectado.[24]

Hacia 1986[25], la Fundación Nacional de Ciencias (NSF, por sus siglas en inglés) comenzó el desarrollo de NSFNET, sucesora de la ARPANET. Originalmente el ancho de banda de su canal de transmisión era de 56 kbs. Actualmente, con el apoyo de la NASA, del Departamento de Energía de los Estados Unidos y de las universidades, es el principal canal de comunicación.

Para 1987, 10,000 servidores anfitriones, estaban conectados a la Red, dos años después el número rebasó los 100,000 servidores y se comercializó la primera versión de Windows, que no fue adoptada de inmediato en el mercado corporativo. La "cara" de la mayoría de las computadoras seguía siendo el sistema operativo DOS (Disk Operating System), también denominado "sistema de interfaz de texto" debido a que el usuario literalmente escribía las instrucciones a ejecutar por la computadora.

[24] Cameron, Deb. “El Internet una Oportunidad de Negocio Global”, Computer Research Corp. Journal, EUA, 1995, p. 136.
[25] Bolio A. Ernesto y Llaguno. Jorge A. Revista Istmo número 250 Septiembre -Octubre del 2000, artículo Creatividad e Innovación en Internet.

Con el fin de administrar e incrementar la capacidad de la Red de la NSF, se garantizó un contrato con MERIT NETWORK INC, IBM Y NCL también en 1987.
En 1990 dejó de existir ARPANET y fue liberado el siguiente gran servicio de la Red: ARCHIE (primer servicio de búsqueda de información en Internet). Al siguiente año apareció el servicio denominado World Wide Web (conocido más por sus siglas "www" que anteceden a la mayoría de las direcciones de Internet), que fue desarrollado por Tim Berners-Lee, del Laboratorio Europeo de Estudios sobre Física de las Partículas (CERN). Berners buscaba facilitar la comunicación entre los científicos que convivían en su laboratorio y desarrolló las bases del lenguaje de marcación de hipertextos (HTML), que permite relacionar frases o elementos de un documento con otros. Su intención era que al accionar una nota a pie de página o una referencia al texto de otro científico, la computadora los llevara al texto fuente de la cita o a la referencia. Pronto se vio la necesidad de relacionar ya no solo citas bibliográficas, sino partes completas de estudios, gráficas, dibujos, fotografías, archivos de sonido... lo que finalmente llevaría al sistema de "navegación a saltos".

En 1991 salió a la venta la versión 3.1 de Windows, que popularizó la Interfaz Gráfica. Para 1992 se alcanzó un millón de servidores en línea y se conectó el Banco Mundial.

Desde 1992, la NSF retiró su inversión, dejando así la posibilidad a otros tipos de financiamiento y, por lo tanto, a otros usos.

En 1993 se conectó a la red la Organización de las Naciones Unidas, también apareció "Mosaic", primer programa para acceder las páginas del servicio "www", ahora conocidos como "navegadores" o "browsers"

A partir de ese momento, el crecimiento en tamaño y tipo de servicios, explotó de manera impresionante. Aparecieron los primeros Centros Comerciales Virtuales y el primer banco que ofrecía sus servicios en línea.

La "www" se convirtió en el servicio más usado, rebasando al servicio de transferencia de archivos (FTP por sus siglas en inglés), anterior monarca en cuanto a la demanda de usuarios. Los sistemas multimedia que permiten ahora manejar textos, datos, audio, imagen y video, han convertido a éste servicio "www" y a su principal vehículo, el lenguaje HTML, en la manera de comunicarse mundialmente.

En 1995, la compañía Sun Microsystems, dio a conocer "JAVA" desarrollo de software que, incluido en los navegadores, permite ejecutar aplicaciones sobre cualquier plataforma computacional, es decir, con cualquier sistema operativo. Ese año se alcanzaron 10, 000,000 de servidores y desde entonces el crecimiento ha sido exponencial[26], alcanzándose en enero de 1999, 40, 000,000 de servidores conectados y más de 1.6 millones de dominios.

También durante la época de los 90', aparecieron los sistemas comerciales de conexión telefónica "dial up" que brindan al usuario doméstico, el acceso a la red mundial, mediante una renta mensual o anual (servicio de ISP, Internet Service Providers). El único límite tecnológico hasta el momento, es la capacidad del medio de transmisión (cableado telefónico en principio y actualmente radio espectro y satélite)

Finalmente, hay que decir que Internet es una federación de Redes que está en constante desarrollo y que, en la actualidad, es de acceso general.

[26] Tasa constante de crecimiento, aplicada durante un periodo.

Después de los investigadores universitarios y de los empleados de instituciones públicas, las compañías privadas y los individuos han visto ahora los beneficios que se pueden obtener viajando a través de las Redes. Antes prohibido, el uso comercial, se ha ido desarrollando con firmeza en los últimos años, contrariamente al espíritu inicial de Internet.

Actualmente, Internet experimenta un crecimiento exponencial y mantiene unidas más de 25,000 Redes por el mundo, que incluyen más de 10,000,000 de servidores y el número de usuarios se estima en más de cuarenta millones.
Total de nombres de dominio registrados en el mundo: 82, 9 a junio del 2006.[27]

Cálculos conservadores estiman que al 30 de junio de 2007 existían aproximadamente 6,574,666,417millones de usuarios de Internet, con el siguiente detalle:[28]

[27] http://www. nua.ie/surveys/
[28] http://www.abcdelinternet.com/stats.htm

### 2.1.1 ESTADÍSTICAS MUNDIALES DEL INTERNET[29]

**(Usuarios del Internet y Población por Países y Regiones)**

| ESTADÍSTICAS MUNDIALES DEL INTERNET Y DE POBLACIÓN | | | | | | |
|---|---|---|---|---|---|---|
| **Regiones** | **Población ( 2007 Est.)** | **% Población Mundial** | **Usuarios, dato más reciente** | **% Población (Penetración)** | **% Uso Mundial** | **Crecimiento ( 2000-2007 )** |
| **África** | 933,448,292 | 14.2 % | **33,545,600** | 3.6 % | 2.9 % | 643.1 % |
| **Asia** | 3,712,527,624 | 56.5 % | **436,758,162** | 11.8 % | 37.2 % | 282.1 % |
| **Europa** | 809,624,686 | 12.3 % | **321,853,477** | 39.8 % | 27.4 % | 206.2 % |
| **Oriente Medio** | 193,452,727 | 2.9 % | **19,539,300** | 10.1 % | 1.7 % | 494.8 % |
| **Norte América** | 334,538,018 | 5.1 % | **232,655,287** | 69.5 % | 19.8 % | 115.2 % |
| **Latinoamérica / Caribe** | 556,606,627 | 8.5 % | **109,961,609** | 19.8 % | 9.4 % | 508.6 % |
| **Oceanía / Australia** | 34,468,443 | 0.5 % | **18,796,490** | 54.5 % | 1.6 % | 146.7 % |

[29] http://www.abcdelinternet.com/stats.htm
NOTAS: (1) Las Estadisticas de Usuarios Mundiales del Internet fueron actualizadas a Junio 30, 2007. (2) Para ver información detallada, de un clic sobre la región o el país correspondiente. (3) Los datos de población se basan en las cifras actuales de World Gazetteer. (4) Los datos de usuarios provienen de información publicada por Nielsen//NetRatings , ITU y de Internet World Stats. (6) Estas estadisticas se pueden citar, siempre y cuando se otorgue el debido credito y se establezca un enlace activo a www.exitoexportador.com . 

| | | | | | | |
|---|---|---|---|---|---|---|
| **TOTAL MUNDIAL** | 6,574,666,417 | 100.0 % | **1,173,109,925** | 17.8 % | 100.0 % | 225.0 % |

### 2.1.2 LOS 10 PAÍSES LIDERES EN EL INTERNET CON MAYOR NUMERO DE USUARIOS[30]

| # | Pais o Region | Usuarios, dato más reciente | Population ( 2007 Est. ) | % Poblacion (Penetracion ) | Fecha dato mas reciente | (%) de Usuarios |
|---|---|---|---|---|---|---|
| 1 | **Estados Unidos** | **210,575,287** | 301,967,681 | 69.7 % | Nielsen//NR Mayo/07 | 18.0 % |
| 2 | **China** | **162,000,000** | 1,317,431,495 | 12.3 % | CNNIC Junio/07 | 13.8 % |
| 3 | **Japon** | **86,300,000** | 128,646,345 | 67.1 % | C.I. Almanac Dic./05 | 7.4 % |
| 4 | **Alemania** | **50,426,117** | 82,509,367 | 61.1 % | Nielsen//NR Junio/07 | 4.3 % |
| 5 | **India** | **42,000,000** | 1,129,667,528 | 3.7 % | IWS - Junio/07 | 3.6 % |
| 6 | **Brasil** | **39,140,000** | 186,771,161 | 21.0 % | ITU - Abril/07 | 3.3 % |
| 7 | **Reino Unido** | **37,600,000** | 60,363,602 | 62.3 % | ITU - Sept./06 | 3.2 % |
| 8 | **Corea del Sur** | **34,120,000** | 51,300,989 | 66.5 % | MIC - Dic./06 | 2.9 % |
| 9 | **Francia** | **32,925,953** | 61,350,009 | 53.7 % | Nielsen//NR Mayo/07 | 2.8 % |
| 10 | **Italia** | **31,481,928** | 59,546,696 | 52.9 % | Nielsen//NR Mayo/07 | 2.7 % |
| | | | | | | |
| **Los 10 Países Lideres** | | **726,569,285** | 3,379,554,873 | 21.5 % | IWS - Junio 30/07 | 61.9 % |
| **Resto del Mundo** | | **446,540,640** | 3,195,111,544 | 14.0 % | IWS - Junio 30/07 | 38.1 % |
| **Total Mundial Usuarios** | | **1,173,109,925** | 6,574,666,417 | 17.8 % | IWS - Junio 30/07 | **100.0 %** |

[30] http://www.abcdelinternet.com/stats.htm
NOTAS: (1) Las Estadisticas de Usuarios del Internet fueron actualizadas a Junio 30, 2007. (2) Para informacion detallada del pais o region, de un clic sobre el pais o region. (3) Los datos de poblacion se basan en las cifras actuales de world gazetteer. (4) Los datos de usuarios provienen de informacion publicada por Nielsen//NetRatings , ITU , Internet World Stats y otras fuentes confiables. (6) Esta informacion se puede citar, siempre y cuando se otorgue el debido credito y se establezca un enlace activo a www.exitoexportador.com . 

De acuerdo con un estudio de Centro del Investigaciones en Comercio Electrónico de la Universidad de Texas[31], la Economía de Internet soporta más de 3 millones de trabajadores en la actualidad, incluyendo 600,000 nuevas posiciones, las cuales se generaron durante el primer semestre del 2000. Esto representa aproximadamente 60,000 trabajadores más de los que emplea la industria de los seguros, así como el doble de las personas empleadas por la industria de bienes raíces.

## 2.2 CARACTERÍSTICAS DE INTERNET

### 2.2.1 ENTORNO SIN FRONTERAS.

La red de redes supone la absoluta libertad de movimientos, la posibilidad de atravesar fronteras sin limitaciones, visados, impedimentos aduaneros. El usuario puede viajar, virtualmente, de un país a otro, adentrándose en otras jurisdicciones, incluso con absoluta ignorancia de que lo hace.[32]

### 2.2.2 INDEPENDENCIA GEOGRÁFICA.

Desde cualquier lugar del mundo se puede teclear en el navegador del ordenador la dirección URL deseada.[33] En una fracción de segundo, el usuario visita páginas

[31] El Centro de Investigaciones en Comercio Electrónico de la Universidad de Texas divulgó su cuarto reporte de Indicadores de la Economía de Internet" en los Estados Unidos. Este reporte mide el crecimiento en puestos de trabajo y en ingresos generados por la Economía de Internet durante el primer semestre del año 2006. Tomado de http://www.vinculodeempresa.com.mx

[32] SVANTESSON, Dan Jerker., pág 45. El autor señala un caso de control de acceso a Internet. En ciertos países con regímenes autoritarios, el acceso a la red se ve intermediado por un proveedor estatal de comunicaciones, al objeto de censurar, previamente, los contenidos que pueden visitar sus ciudadanos.
La República Popular China, considerando el peligro que representaba Internet se anticipó dictando las Provisonal Regulations of the People's Republic of China for the Administration of Internacional Connections to Computer Infomration Networks (1997)

[33] 16 URL significa Uniform Resource Locator, es decir, localizador uniforme de recurso. Es una secuencia de caracteres, de acuerdo a un formato estándar, que se usa para nombrar recursos, como documentos e imágenes en Internet, por su localización.

web localizadas en distintos lugares del planeta. Si la navegación transcurre con normalidad, el internauta comprobará como, independientemente de que la página visitada se encuentre en su propio país o en las antípodas, la velocidad de conexión es prácticamente la misma (instantánea), no siendo un elemento determinante la medición tradicional de las distancias.

### 2.2.3 INDEPENDENCIA DE LENGUAJE.

Al contrario que los sistemas de comunicación precedentes (teléfonos, radiofonía, telégrafo, etc.), la World Wide Web, por medio de una sofisticada tecnología, posibilita el acceso multilingüe a las páginas visitadas. Ello permite, a través de aplicaciones ofrecidas por diferentes operadores, que cualquier persona se incorpore a Internet sin mayores impedimentos. Se desarrolla asimismo un sistema peculiar de comunicación, una jerga propia de internautas.[34]

### 2.2.4 PERMITE LA COMUNICACIÓN DE UNO A MUCHOS (ONE-TO-MANY COMMUNICATIONS.)

Esta característica es trascendental y utiliza la tela de araña para que los efectos de su acción se multiplique a multitud de personas.

### 2.2.5 SISTEMA INCOMPARABLE DE DISTRIBUCIÓN DE INFORMACIÓN.

Ni la televisión ni la radio ni, por supuesto, los sistemas de comunicación predecesores poseen la fuerza distributiva de la WWW. Cualquier persona, con escasos medios técnicos y financieros, puede entrar el circuito y utilizar la red para

---

Las URL fueron una innovación fundamental en la historia de Internet. Fueron usadas por primera vez por Tim Berners-Lee en 1991, para permitir a los autores de documentos establecer hiperenlaces en la World Wide Web (WWW o Web). Desde 1994, en los estándares de Internet, el concepto de URL ha sido incorporado dentro del más general de URI (Uniform Resource Identifier - Identificador Uniforme de Recurso), pero el término URL aún se utiliza ampliamente. www.webopedia.com/TERM/U/URL.html y http://es.wikipedia.org/wiki/URL.

[34]Consultada la vigésima segunda edición del Diccionario de la Real Academia de la Lengua (2001) (http://www.rae.es) se define la página web como “Documento situado en una red informática, al que se accede mediante enlaces de hipertexto.” Nuestro diccionario todavía no ha incorporado palabras como internauta, ciberdelito, cibercrimen, ciberdelincuente, website y otras que, nosotros, por necesidades explicativas habremos de utilizar frecuentemente.

difundir sus opiniones, investigaciones, filosofías y doctrinas. Las posibilidades de delinquir aumentan exponencialmente.

### 2.2.6 AMPLIAMENTE UTILIZADO, CADA DÍA MÁS.

En pocos años la difusión de Internet ha llegado a casi todos los hogares de los países desarrollados.[35] En países subdesarrollados el uso se incrementa, sin que la precariedad de la economía sea un obstáculo insalvable. Países en vías de desarrollo, como India y Filipinas, se sitúan a la cabeza mundial en los avances informáticos relacionados con Internet.[36] El acceso a tal tecnología y, es abierta y popular.

### 2.2.7 PORTABILIDAD.

El fenómeno de la WWW se caracteriza por la ubicuidad. La irradiación de los contenidos es altamente escurridiza, pudiendo situarse, aunque los contenidos distribuidos sean idénticos, en varios puntos del planeta. Esto obedece a diversos motivos, que pueden ser lícitos (simplemente para facilitar los accesos o la velocidad de descarga) o ilícitos (situarse fuera del alcance de la persecución policial o judicial.) Así, una página Web puede ser reflejada (por medio de mirrors) en un servidor localizado en cualquier otro lugar del planeta, con el simple objeto de distribuir los accesos – sin saturar las bandas – y aumentar la velocidad al usuario, que se ve, de esta forma, favorecido por un mejor servicio.

---

[35] El número de personas que han utilizado Internet en España en los últimos tres meses del año, ha pasado de 13.534.664 en el año 2004 a 15.131.420 en el año 2005. Fuentes: Asociación Española de Usuarios de Internet. Disponible en: http://www.fundacionauna.org/areas/25_publicaciones/eEspana_2006.pdf.

[36] Precisamente países como Filipinas o India suelen ser el origen de perniciosos virus, sorprendiendo a las propias autoridades que no encontrar fundamento legal alguno para entablar acciones criminales contra sus autores. Puede destacarse el virus "I Love You" programado por el estudiante filipino Onel de Guzmán que fue desatado el 4 de mayo de 2000 causando daños por unos 8.7 billones de dólares. Vid. EVANS, James. "'Love Bug' Suspect Charged". *PC WORLD.* Disponible en http://www.pcworld.com/article/id,17497-page,1/article.html.

Por las mismas razones (excelencia en el servicio) es tecnológicamente posible que el texto de una página Web se aloje en un servidor y las imágenes en otro, convergiendo en el navegador del usuario textos e imágenes perfectamente editadas y maquetadas. El internauta desconoce la procedencia del contenido –tal vez de distintos Estados pero se contenta con el acceso más veloz.

A semejanza de las antiguas fondachi o las alhóndigas que albergaban a los navegantes, es curioso que en ciertos aspectos –en el de la inversión de la responsabilidad, en el de la ubicación, etc.— el servidor se convierta en un establecimiento extraterritorial. Una suerte de incubadora, necesaria para la propagación de la Sociedad de Información, pero que debe involucrar al Derecho Público por ser la necesaria plataforma desde donde cometer los delitos.

Estas „alhóndigas de comerciantes" son las denominadas server farms, emporios cibernéticos donde las empresas alojan sus páginas Web. El server farm, a cambio de una retribución, provee de electricidad, de ancho de banda para conectarse y del espacio físico para alojar los contenidos (espacio en el disco duro.) Una versión del server faro es el Internet content host.

Este servidor, además de los servicios facilitados por el Server farm, suministra efectivos servidores y pueden también acometer el mantenimiento eficaz de las websites. Tanto en uno como en otro caso, el sistema de websites se aloja en „barns", especie de graneros o viveros donde se hospedan billones de datos binarios y que poseen una sede física situada en un Estado determinado, que puede no coincidir –y normalmente no coinciden—con la empresa que ha contratado el servicio. Al objeto de nuestro análisis esta cuestión no es baladí pues origina conflictos de jurisdicción y competencia, como se verá más abajo.

### 2.2.8 FALTA DE IDENTIFICADORES SEGUROS.

La carencia de identificadores seguros se manifiesta en dos sentidos, tanto desde la perspectiva del que remite la información, como desde el punto de vista de

quien recibe la información. Ambos agentes de la comunicación en la WWW carecen de medios fiables para identificar a sus respectivos interlocutores.

El usuario corriente de la WWW sólo conoce, como máximo la dirección IP[37], y el nombre de dominio, conocido com DNS[38]. Algunos nombres de dominio contienen identificadores geográficos, dominios de nivel superior nacionales (ccTLD), basados en la nomenclatura ISO 3166. Sin embargo, esta nomenclatura es equívoca porque websites de un país pueden utilizar códigos de otros países[39]. Así muchos websites suecos emplean el código .nu de Niue, ya que nu significa en sueco „ahora". La identificación es aun más difícil cuando se utilizan dominios de nivel superior genéricos (gTLDs) El problema se acentúa cuando hablamos de dominios de segundo nivel.

Si bien comienzan a desarrollarse las denominadas geo-location tecnologies, consistentes en medios técnicos que conectan una dirección IP con un emplazamiento físico, todavía estas tecnologías no son fiables y se hallan escasamente implantadas.[40]

[37]Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar. Vid. http://www.webopedia.com/TERM/I/IP.html y http://es.wikipedia.org/wiki/Ip.

[38] El DNS se traduce en una base de datos jerárquica, en cuyo vértice figura el dominio raíz ".", a partir del cual brotan una serie de dominios de nivel superior (TLDs). Éstos se dividen, a su vez, en genéricos y nacionales. Los primeros (gTLD) incluyen tanto las extensiones tradi-cionales como .com, .net, .org, así como las más recientemente aprobadas por la ICANN, como .name, .biz o .pro. Por su parte, los segundos (ccTLD), hacen alusión a los dominios asociados a países específicos, como .fr (Francia), .br (Brasil) o .cr (Costa Rica), representados por dos caracteres correspondientes al código ISO-3166 de cada nación. Clara explicación ofrecida por HESS ARAYA, Christian. "El nombre de dominio, ¿una nueva forma de propiedad?". Publicación electrónica disponible en http://www.hess-cr.com/secciones/dereinfo/ dnspropiedad.shtml, visitado el día 11 de noviembre del 2005. San José de Costa Rica, 2002.

[40]Su implantación definitiva originará la eterna controversia seguridad versus intimidad, que animará encendidos debates que no son objeto de este trabajo.

Esta característica consustancial de la WWW añade el problema de las dificultades perseguibilidad (investigación cibernética) y la efectiva punición de las conductas antijurídicas.

### 2.2.9 INEXISTENCIA DE UNA AUTORIDAD CENTRAL QUE CONTROLE EL ACCESO A LA WWW.

Paralelamente al surgimiento de Internet, se inició un arduo debate sobre la necesidad de regulación del fenómeno. . Los ensayos normativos en nuestra legislación (tanto nacional como transnacional)[41] han merecido vehementes críticas, no sólo desde sectores no intervencionistas o antiglobalización, sino también desde posturas estrictamente técnicas[42].

En un escenario tan complejo como el de Internet, el Derecho se ve desbordado ante la celeridad tecnológica, achicando tempestades mediante tímidas respuestas, varando en instrumentos jurídicos antiguos. El acervo precedente hace que las adaptaciones sean incompletas. Realmente se ha creado una superestructura que requiere pilares y planteamientos también novedosos, sin que se encuentren absolutamente condicionados por el pasado. Los juristas se ven impotentes para comprender la problemática tecnológica y prever los avances que se avecinan. Para colmo, una vez comprendidos éstos, los instrumentos normativos se elaboran lentamente: cuando se promulgan están llamados a regir poco tiempo, pues pronto se quedan obsoletos.

[41] En especial, la Ley 34/2002, de 11 de julio, sobre servicios de la sociedad de la información y de comercioelectrónico, que traspone al ordenamiento jurídico interno la Directiva 2000/31/CE del ParlamentoEuropeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico.)

[42] Sánchez Almeida, Carlos. (2004, Marzo). Ponencia presentada en el XIII Congreso de responsabilidad Civil, organizada por la Comisión de Abogados de Entidades Aseguradoras y Responsabilidad Civil del Ilustre Colegio de Abogados de Barcelona. *República Internet.* Consultada el 29 de septiembre de 2005, http://www.tercerarepublica.com/articulo.php?id=25

La regulación de Internet, en consecuencia, siempre estará plagada de lagunas. Estas lagunas se deben llenar con autorregulación, por lo menos, en tanto que no exista una norma positiva.

La costumbre, fuente del Derecho, se va a caracterizar en Internet por una rápida conformación (lo que, en cierto modo, contradice el concepto mismo de costumbre.) La introducción de nuevos elementos en la red, amparados por la libertad de prestación de servicios[43], a los que el Derecho no puede responder con la misma rapidez, fomenta el nacimiento de una costumbre "Express". Los usos, que conceptual y tradicionalmente, tardaban años en gestarse, ahora tardan meses, por la propia necesidad de autorregulación.

Ante este panorama, caracterizado por una autorregulación de facto, sólo podrá existir un control meramente tecnológico y de naturaleza privada. Los ISP pueden controlar el acceso de sus usuarios, pero desde una perspectiva técnica sin que le sea permitido un juicio de contenidos, más allá de uno somero y grueso.

Algunos gobiernos podrían legislar sobre el comportamiento en Internet de sus ciudadanos, pero la contravención de tales normas difícilmente se podrían castigar, por las dificultades de investigación ya señaladas más arriba.

## 2.3 DESARROLLO DEL INTERNET

Primeramente debemos saber: ¿Qué es el Internet?

En este punto podríamos decir es la red de redes o la autopista de la información, la mayor red de computadoras de la historia, el caber espacio, todos ellos términos difusos e imprecisos utilizados hasta el hartazgo por infinidad de

[43] Se proclama el principio de la no sujeción a autorización previa para la prestación de servicios en la Sociedad de la Información, salvo ciertos supuestos (véase el art. 6 de la Ley 34 de España , sobre servicios de la sociedad de la información y de comercio electrónico.)

publicaciones. En nuestro caso, procurando brindar un rasgo de originalidad recurriremos a la precisión de definiciones reconocidas.

### 2.3.1 SEGÚN LA FUNDACIÓN NACIONAL DE CIENCIA (NSF)[44]

El consejo federal de interconexiones (Consejo Federal de Redes). Manifiesta que las siguientes expresiones reflejan la definición de Internet.

INTERNET se refiere al sistema de información global que:

1. se encuentra vinculado lógicamente por un espacio direcionable global determinado, basado en el protocolo de Internet (ip) o sus subsecuentes extensiones y agregados.
2. Es capaz de soportar comunicaciones utilizando el conjunto de herramientas del Protocolo de Control de Transmisiones/ Protocolo de Internet (TCP/IP) o sus subsecuentes extensiones y agregados.
3. Provee, utiliza o hace accesible, sea en forma pública o privada, servicios de alto nivel estratificados en las comunicaciones y la infraestructura.

### 2.3.2 SEGÚN LA SOCIEDAD DE INTERNET[45]

La Internet es una red global de redes que posibilita a computadores de todo tipo comunicarse en forma directa y transparente y compartir servicios a través de la mayor parte del mundo. Por ser la INTERNET un enorme activo permitiendo capacidades para tantas personas y organizaciones; también constituye un recurso global compartido de información, conocimiento y medios de colaboración y cooperación entre incontables diferentes comunidades.

### 2.3.3 Y PARA OTROS

[44] El 24 de octubre d e1995 la NSF emitió resolución definitoria redactada con miembros vinculados al desarrollo de Internet y comunidades de Derecho de la Propiedad Intelectual.
[45] Ver http://www.iso.org

La respuestas pueden ser muy variadas, dependiendo del tipo de gente que utiliza este medio de comunicación; para algunos, Internet no es más que un medio para comercializar y difundir productos; para otros, es una fuente mundial de información con acceso a bases de datos de todo el mundo; mientras que para otros tantos más, es un medio de expresión de ideas.

Las características fundamentales de la operación de Internet consisten en que se trata de una red **distributiva** (no cuenta con un depósito central de información o de control, sino que está compuesto por una serie de computadoras host o anfitrionas que están interconectadas, cada una de las cuales puede ser accesada desde cualquier punto de la red en que el usuario de Internet se encuentre), **ínter operable** (utiliza protocolos abiertos, de manera que distintos tipos de redes e infraestructura puedan ser enlazados, permitiendo la prestación de múltiples servicios a una diversidad de usuarios a través de la misma red. En este sentido, la interoperatividad con la que cuenta Internet se debe al protocolo *TPC/IP*, el cual define una estructura común para datos de Internet, así como para el enrutamiento de dichos datos a través de la red) y que funciona a través **de transferencias de paquetes de información** (mejor conocida como conmutación de paquetes, consistente en dividir la información que se transmite por la red en pequeñas partes o paquetes).

En términos generales, podemos decir que Internet, es un canal mundial de telecomunicaciones informáticas, que está integrado por muchos canales que a su vez, están interconectados entre sí, lo cual lo convierte en el medio de comunicación más veloz en toda la historia de la humanidad.
Como comentamos en el capítulo anterior, Internet fue creado hace aproximadamente 30 años por el Departamento de Defensa de los Estados Unidos de América como un canal experimental diseñado como un medio de apoyo en la investigación militar.

En esa época, se le denominaba ARPANet (Agencia para Proyectos de Investigación Avanzada), sin embargo, con el paso del tiempo, se fueron desarrollando paralelamente otros canales similares, como el establecido por la Fundación Nacional de Ciencias para permitir a los estudiantes y universidades acceder al ARPANet con fines educacionales.[46]

Poco a poco, ha ido aumentando el número de los canales que se han conectado al ARPANet, a tal grado que actualmente las grandes empresas mundiales y los individuos considerados como personas físicas, están descubriendo y explorando el mundo de Internet.

Este proceso de comunicación global, ha sido estimulado por inventos tales como el teléfono, el telégrafo, el fax y las telecomunicaciones, encontrándonos actualmente en la era de la computación y de las comunicaciones por este medio.

Desde sus comienzos, esta Red de canales conocida como Internet, ha crecido hasta el punto de englobar a más de seis millones de canales interconectados con Internet y a más de cuarenta millones de usuarios en todo el mundo, entre los que podemos incluir agencias gubernamentales, universidades, investigadores, compañías privadas e individuos personas físicas.

Sin embargo, dentro de los múltiples fines citados que los usuarios dan actualmente a la Red, el más importante para fines jurídicos, es el del comercio a través de Internet, dado que las compañías tanto privadas como del sector público de diversos países, han visto los beneficios que Internet está aportando al comercio mundial, y los futuros beneficios que aún no se han aprovechado por falta de conocimientos plenos y de una regulación jurídica apropiada para las

[46] Kahin, Brian, Keller, James “Acceso Publico al Internet”, Instituto de Tecnología Press, p. 136, 1996.

transacciones realizadas a través de la Red.

Un sistema avanzado para el comercio electrónico como el que constituye Internet, puede comprender actividades tales como:
Transferencias electrónicas de fondos.
Regulación gubernamental de intercambio de datos.
Colaboración técnica entre pases o industrias.
Integración de consorcios.
Soporte computacional para la colaboración en el trabajo.

El comercio electrónico puede combinar las ventajas de las computadoras (velocidad, rentabilidad y gran volumen de datos), con las ventajas de las personas (creatividad, flexibilidad, adaptabilidad), para crear un entorno de trabajo con mayor dinamismo y rapidez en las operaciones comerciales, además de permitir a las personas revisar, analizar, añadir valor y vender, una gran gama de productos y de servicios a nivel mundial que están representados electrónicamente a manera de catálogos, materiales de referencia, libros de texto y materiales de entrenamiento, apoyo y software.[47]

En resumen, el comercio electrónico difiere del comercio tradicional básicamente en la forma en que la información es procesada e intercambiada, ya que, tradicionalmente, la información es intercambiada directamente, a través del contacto directo entre personas o a través del uso de teléfonos o de sistemas postales, mientras que el comercio electrónico maneja la información por la vía digital de los canales de comunicaciones y sistemas de cómputo.

Como resultado del incremento en el uso de Internet, muchas compañías temen que sus respectivos gobiernos impongan extensivas y represivas regulaciones en

[47] Fernández Flores, Rafael, "La WWW una telaraña que se teje a plena luz del día", en la revista RED, no. 70, año VI, pp. 38-40, julio de 1996,

Internet y por lo tanto en el comercio electrónico, sin embargo, es precisamente durante esta época de auge del comercio electrónico, cuando debe de establecerse una regulación adecuada que permita la seguridad jurídica en las transacciones realizadas en la Red, sin embargo, esto requiere de un esfuerzo a nivel mundial por parte de los gobiernos de los distintos países usuarios de Internet, pero este tipo de esfuerzos se encuentra todavía en un nivel incipiente.

Son precisamente los gobiernos, quienes pueden tener un profundo efecto en el desarrollo del comercio en Internet. Con sus acciones ellos pueden facilitar el comercio en Internet o inhibirlo, pero para ello, deben de tener siempre en cuenta la propia naturaleza de la RED como un medio de comunicación mundial que se ha venido desarrollando en un marco esencial de libertades que no pueden ser cortadas de tajo, porque si esto llegara a ocurrir, se generaría un proceso de virtual abandono de este medio de comunicación.

Un buen desarrollo de la RED, estimula las aplicaciones del comercio electrónico y sus beneficios entre los cuales podemos encontrar los siguientes:

- ✓ Desaparecer los límites geográficos.
- ✓ Estar disponible las 24 horas del día, 7 días a la semana, todos los días del año.
- ✓ Reducción de un 50% en costos de la puesta en marcha del comercio electrónico, en comparación con el comercio tradicional.
- ✓ Hacer más sencilla la labor de comunicación y negociación.
- ✓ Reducción considerable de inventarios.
- ✓ Proporcionar nuevos medios para encontrar y servir a clientes.
- ✓ Incorporar internacionalmente estrategias nuevas de relaciones entre clientes y proveedores.
- ✓ Reducir el tamaño del personal de la fuerza.
- ✓ Menos inversión en los presupuestos publicitarios.

- ✓ Reducción de precios por el bajo coste del uso de Internet en comparación con otros medios de promoción, lo cual implica mayor competitividad.
- ✓ Cercanía a los clientes y mayor interactividad y personalización de la oferta.
- ✓ Desarrollo de ventas electrónicas.
- ✓ Globalización y acceso a mercados potenciales de millones de clientes.
- ✓ Implantar tácticas en la venta de productos para crear fidelidad en los clientes.
- ✓ Enfocarse hacia un comercio sin el uso del papel, lo cual es posible a través del EDI.
- ✓ Bajo riesgo de inversión en comercio electrónico.
- ✓ Rápida actualización en información de productos y servicios de la empresa (promociones, ofertas, etc.).
- ✓ Obtener nuevas oportunidades de negocio, con la sola presencia en el mercado.
- ✓ Reducción del costo real al hacer estudios de mercado.
- ✓ Un medio que da poder al consumidor de elegir en un mercado global acorde a sus necesidades.
- ✓ Brinda información pre-venta y posible prueba del producto antes de la compra.
- ✓ Inmediatez al realizar los pedidos.
- ✓ Servicio pre y post-venta on-line.
- ✓ Reducción de la cadena de distribución, lo que le permite adquirir un producto a un mejor precio.
- ✓ Mayor interactividad y personalización de la demanda.
- ✓ Información inmediata sobre cualquier producto, y disponibilidad de acceder a la información en el momento que así lo requiera. y,
- ✓ Reduce el uso de materiales que dañen el medio ambiente a través de la coordinación electrónica de actividades y el movimiento de información en vez de objetos físicos.[48]

[48] Tecnología de la infraestructura de la información y grupo de tarea de los usos (UTA), Oficina Nacional de la Coordinación para el High Performance Computing and, February 1994, pp. 13.

Muchas compañías en distintas ramas de la industria, han experimentado los beneficios y encontrado, la necesidad del uso del comercio electrónico para sobrevivir.

Como se ha visto anteriormente, muchas compañías y agencias gubernamentales usan las aplicaciones del comercio electrónico para facilitar sus operaciones internas e interactuar con mayor eficiencia con las demás entidades comerciales.

Con una extensa gama de transacciones electrónicas, el desarrollo de las aplicaciones del comercio electrónico, requiere una gran estructura comercial, el establecimiento previo de arreglos y por otra parte, líneas dedicadas a ello o canales de valor agregado.

Lo anterior, permite ver que muchas veces, la necesidad de contar con cierta infraestructura para integrarse al comercio electrónico, crea barreras para la inversión y gastos excesivos, sobre todo para la pequeña y mediana empresa.

Sin embargo, a pesar de estas barreras, el mercado electrónico se consolida a paso rápido. Para finales de 1994, más de 10,000 compañías ofrecían información y servicios a la venta en una combinación de Internet y canales de Valor Agregado.[49]

Actualmente, podemos percibir la gran influencia que tiene Internet en todos los ámbitos de la vida social, las referencias a la Red son incrementadas frecuentemente en los medios tradicionales de publicidad, como carteles y anuncios televisivos en los que aparece la conocida expresión "http://www." la cual parece incrementar su aceptación por los consumidores como una referencia a un

[49] Emery, Vince, “Como crecer su negocio en la red”, p. 82, Edit. Coriolis Group/IDG,1996.

sitio en la Red, el cual provee mayor información sobre una compañía particular y sobre sus productos y servicios.

Quitando el hecho de que una página local (HOME PAGE) o sitio en la Red (WEB SITE) puede ser accesado simultáneamente y sin restricción por potenciales compradores en cualquier número de jurisdicciones, los problemas que afectan la publicidad en Internet, no difieren substancialmente de los que afectan la publicidad en los medios tradicionales.

Nos encontramos además, con problemas de tipo civil y penal. En cuanto a los problemas de tipo civil, nos referimos especialmente al problema de la contratación jurídica por medios electrónicos, específicamente, por Internet, partiendo de la definición del entorno general de la RED en que se lleva a cabo la contratación, así como de las circunstancias de tiempo y lugar que afectan la vida de dicho contrato y su validez, así como los problemas jurisdiccionales a que puede dar lugar el incumplimiento e interpretación de un contrato celebrado a través de Internet, sin dejar de considerar la falta de seguridad jurídica reinante en el medio, a falta de la existencia de un marco jurídico adecuado que permita la regular la celebración de negocios y transacciones.

Otro aspecto que podemos mencionar, es el que se refiere al campo del derecho penal, ya que la RED, al igual que todos los medios y ámbitos de la vida social, es un medio que se presta para la comisión de diversos tipos de delitos utilizando esta forma de comunicación y de transferencia de datos, a los que en el propio medio de Internet se les ha dado la denominación de "Cibercrímenes" y la persecución de éstos, ese aspecto se tratará muy someramente en la parte relativa a novedades legislativas en el presente trabajo.

Como se mencionó antes, Internet es una fuente de problemas en cuanto a su reglamentación jurídica, ya que diversos aspectos del derecho se encuentran íntimamente vinculados a este medio.

Cabe también destacar, que se ha concebido la idea de la creación de una página que permita a todos los usuarios de la RED, el acceso y conocimiento de las leyes y códigos sobre publicidad en Internet, sin embargo esto implica un esfuerzo a nivel mundial que nadie ha estimulado.

Lo anterior es de suma importancia, si se toma en cuenta que a una transacción realizada a través de Internet, se le da un distinto tratamiento jurídico en cada país, por ejemplo, por lo que respecta a la propiedad intelectual, en Alemania la oferta de "muestras" gratis por sí misma puede, en ciertas circunstancias, constituir una violación al Código Civil que rige la publicidad en dicho país.[50]

Igualmente el anunciarse como el "líder del mercado", puede causar problemas en Alemania y ciertamente la comparación con el producto del rival, puede ir en contra del Acta Alemana de Competencia desleal.

Mientras que en Italia, la jurisprudencia se ha desarrollado en el sentido de que el público no es fácilmente engañado por las exageraciones en la publicidad y generalmente no toma los anuncios muy seriamente.

Como otro ejemplo, en Francia toda la literatura de mercadeo y ventas debe, técnicamente, estar en francés, sin embargo, ¿cómo hacer compatible este requerimiento de la ley francesa y cómo interpretarlo en la práctica al conectarse

[50] Graham Alian, Baker & McKenzie, Comercio Electrónico: Contrataciones el Ciberespacio, p. 4, Londres, Octubre 1996, en: www.bakerinfo.com

con los sitios locales de la RED en servidores fuera de Francia?, éste es un problema aún no resuelto.[51]

Además, hay otra serie de problemas que hay que considerar en torno a Internet: Tanto el gobierno como las industrias no pueden aceptar el comercio electrónico sin que las transacciones electrónicas sean seguras. Hay una clara necesidad de autenticación de la fuente de la transacción, de verificar la integridad de la transacción, la prevención de la intervención de usuarios no autorizados en la transacción y la verificación de recibo de la transacción para el otro contratante. ¿Es el actual trabajo de los sistemas de seguridad en computación, adecuado para la pronta resolución de estos problemas técnicos o la dirección de este trabajo debe ser modificada o el esfuerzo incrementado? ¿Qué organizaciones y mecanismos se necesitan para asegurar que el gobierno y la industria pueden resolver estos problemas de seguridad mencionados?

La aplicación del comercio electrónico requiere ínter operación de comunicaciones, proceso de datos y servicios de seguridad. Estos servicios serán proveídos por diferentes compañías; pero dada esta diversidad, ¿cómo pueden el gobierno y la industria asegurar que el comercio electrónico será rentable, y que los componentes pueden ser ensamblados, mantenidos y mejorados a un costo razonable? se deben desarrollar tecnologías, herramientas, servicios de prueba, demostraciones de interoperabilidad, etc. para asegurar que un componente satisface los actuales y los futuros requerimientos del gobierno y de la industria.

La solución de problemas técnicos, será insuficiente para asegurar el uso apropiado del comercio electrónico; las barreras de tipo económico, cultural, regulatorias y legales al comercio electrónico deben ser identificadas y removidas, por ejemplo: ¿cómo puede el gobierno y la industria asegurar que el comercio

[51] IBIDEM, P. 5.

electrónico será visto positivamente por los trabajadores?, ¿Qué incentivos pueden ser usados para que los trabajadores participen de los beneficios del comercio electrónico?, ¿Cómo puede el gobierno y la industria establecer casos realistas de negocios e historias exitosas para motivar a los potenciales usuarios y proveedores del hardware, software y servicios para el comercio electrónico?

## 2.4 PROBLEMÁTICA GENERAL EN EL INTERNET

Existen grandes facilidades y alcances que el comercio electrónico ofrece, pero también podemos encontrar diversas problemáticas, principalmente el de la seguridad y la confiabilidad en el comercio electrónico.

Tradicionalmente el documento por escrito, ha sido la prueba por excelencia de las convenciones o negocios jurídicos, pero no la única, pues nada impide que la voluntad de contratar o extinguir una relación jurídica, sea acreditada a través de otros medios de prueba.

Ya que no en todos los casos el usuario puede solicitar el envió físico del contrato que documenta la transacción, esto ocurre entre usuarios separados por grandes distancias, es de mencionar el hecho de que en la mente de un comerciante la exigencia del documento en papel atenta contra la celeridad de las transacciones electrónicas que él ofrece, ya que esta desmaterialización es una práctica del Comercio Electrónico, derivada de las ventajas de reducción de costos, por lo que se busca que las personas obvien los documentos escritos.

Hoy en día, este problema ha tenido una solución gracias al comercio electrónico, donde se desmaterializan los documentos escritos. Además cabe enunciar que la seguridad en este medio lleva ciertos riesgos, tanto en el sistema como en el dato, a la posibilidad de alteraciones o destrucciones de datos informáticos, es decir a la violación de la confidencialidad e integridad y disponibilidad de la información.

Evidentemente, esto abre las puertas a muchos tipos de fraude: falsificación de mensajes y cartas, modificación maliciosa de las condiciones de los contratos, o suplantación de personalidad, por citar sólo algunos.

Además, la confiabilidad de la información obtenida, puede también ser materia de riesgo.

De ahí que sea necesaria la creación de diversos mecanismos de verificación de la información.

Según Rosa Julia Barceló y Thomas Vinje: ***"El crecimiento del Comercio Electrónico depende de la capacidad de los mensajes electrónicos para ser confidenciales y seguros"***[52]; en virtud de que los mensajes y documentos electrónicos constituyen la forma en que los comerciantes y usuarios de los medios electrónicos realizan la mayoría de sus transacciones comerciales.

En la actualidad los Estados tienen la necesidad de obtener un medio confiable que se vea reflejado en tratados bilaterales, legislaciones internas o la enunciación sobre autentificación, integridad y confidencialidad de la información, encontrando como mecanismo a utilizar la Firma Electrónica.

[52] Barceló, Rosa Julia y Vinje Thomas, Hacia un marco europeo sobre firmas y criptografía. Revista de Derecho Mercantil. Número 228, Abril-Junio, 1998. Madrid. www.vlex.com.

# CAPITULO III

## 3.0 DE LAS FIRMAS

## 3.1 ORIGEN DE LA FIRMA

El vocablo firma proviene latín *firmare* que significa: afirmar, dar fuerza y el vocablo *autógrafa* significa: grabar o escribir por sí mismo, y se aplica al escrito de mano de su propio autor en el entendido que los signos o trazos han de ser hechos por la mano del autor sin que la impresión se realice por medios mecánicos.[53]

La Real Academia de la Lengua define la firma como: “nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice”.

Para *Couture* se define como: “Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice”

Existen rasgos de primeras escrituras, como sabemos desde la prehistoria, y en culturas muy antiguas, en las que destacan *Súmenos, Cretenses*, y los alfabetos egipcio, fenicio y griego son pruebas destacadas del adelanto de dichas civilizaciones.

En Roma, los documentos no eran firmados, ni era costumbre ni era necesario. Existía una ceremonia llamada *manufírmatio*, por la cual, luego de la lectura del documento por su autor o el *notarius*, era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir esta ceremonia se estampaba el nombre del autor, signo o tres cruces una por cada persona de la Santísima Trinidad, haciéndolo seguidamente los

[53] “Firma" Enciclopedia Jurídica Omeba, Tomo XII, Editorial Bibliográfica Argentina, pp. 290-293

testigos. Más que un requisito la *manufírmatio* era en sí misma una parte del espectáculo solemne en que se realizaba el acto.[54]

En el Sistema Jurídico Visigótico[55] existía la confirmación del documento por los testigos que lo tocaban *"chartam tangere"*, signaban o suscribían *(fírmatio, roboratio, stipulatio)*. La firma del que da el documento o librador es corriente, pero no imprescindible. Los documentos privados son, en ocasiones, confirmados por documentos reales. Desde la época e*uriciana* las leyes visigodas prestaron atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escrituras. La *"subscriptio"*, representaba la indicación del nombre del signante y la fecha, y el *"signum"*, un rasgo que la sustituye si no sabe o no puede escribir. La *"subscriptio"* daba pleno valor probatorio al documento y el *"signun"* debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, éste es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido.[56]

En la Edad Media se utilizaron sellos, marcas y signos. Estos últimos se formaban con una cruz con la que se entrelazaban, en forma arbitraria, letras o rasgos y fueron utilizados por nuestros fedatarios hasta hace no mucho tiempo. Carlo Magno que apenas sabía escribir hacia firmar sus actos por un sellero oficial, sus sucesores que no mejoraron la cultura del conquistador, utilizaron sellos, hasta que algún tiempo después comenzaron a autenticarse los documentos con sello y firma aunque por esto se entendían todavía los signos dibujados para individualizarse.[57]

---

[54] FLORIS MARGADANT G. "Derecho Privado Romano" 4a ed. Editorial Porrúa. pp. 116-119

[55] Se define como el conjunto de instituciones y legislación que se desarrolla en la península Ibérica desde el siglo V hasta al VII. Como fecha inicial podemos citar el año 409, año en el que penetra en la hispania los diversos pueblos de origen germano, como suevos, vándalo y alanos

[56] TOMAS Y VALIENTE FRANCISCO "El orden Jurídico Medieval" Madrid, Marcial Pons, Ediciones Jurídicas y Sociales, S.A. pp. 53-54

[57] ídem.

Recién en octubre de 1358, Carlos V obligó en Francia a los escribanos a suscribir los actos que pasaban ante ellos con sus firmas, además de sus signos. Era en esta época aún tan poco común la escritura, que ese mismo año, en el Consejo Real eran escasos los que sabían hacerlo, y fue por entonces que el mismo rey dispuso que los actos de ese organismo debían de ser autorizados por lo menos por tres de los presentes, los que si no supiesen firmar estamparían sus marcas o signos.

La diferenciación entre “firmas” y “signos” hizo que se empezase a entender que aquéllas eran, más que simples “signos”, la inscripción manuscrita del nombre o de los apellidos. En ese tiempo, pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban en los documentos que suscribían diversos signos o sellos, la extensión de la instrucción y el desenvolvimiento de las transacciones comerciales, hicieron que la firma fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.[58]

Es así como la firma se utilizó con mucha frecuencia por los artistas, son célebres las firmas por ejemplo de Alberto Durero, que más bien es un signo, o la de Miguel Ángel que especialmente firmó algunas de sus obras que consideró más significativas.[59]

Los artistas chinos usan su firma para distinguir sus obras, ya sean de pintura, escultura, bordado, porcelana, etc., y es famosa en el mundo entero la firma de

[58] ACOSTA ROMERO, Miguel; "Nuevo Derecho Mercantil"; capítulo XVIII: La firma en el derecho mercantil mexicano; página 537 a 562; Editorial Porrúa; Primera Edición; 15 de agosto del 2000.
[59] ACOSTA ROMERO, Miguel; OP. CIT.

estos grandes artistas que se significa por su perfección en el trazo y que se estampa en color rojo.[60]

### 3.2 CONCEPTO

La firma puede definirse de la siguiente manera: *"Nombre, apellido o titulo que se pone al pie de un escrito para acreditar que procede de quien lo escribe, para autorizar ahí lo manifestado u obligarse a lo declarado en el documento"*[61], es decir que se trata de un rasgo o conjunto de rasgos gráficos, que tienen existencia desde que el sujeto las emplea como individualización; y demostrar su presencia, propiedad, titularidad o autoría del documento al que se incorpora.

Como una primera aproximación, podemos decir que Firma es el conjunto de letras y signos entrelazados, que identifican a la persona que la estampa, con un documento o texto.
La firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto.

*Mustapich*[62] define a la firma: "El nombre escrito por propia mano en caracteres alfabéticos y de una manera particular, al pie del documento al efecto de autenticar su contenido".
*Planiol y Ripert*[63] consideran: "La firma es una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto".

La definición de *Mustapic*h no concuerda con la realidad actual, al afirmar que la firma es el nombre escrito por propia mano en caracteres alfabéticos, pues quedarían fuera de esa definición las firmas que se componen exclusivamente de

[60] Bradley Smith y Wan-go Wen, China Historia en Arte. Editorial Windfall & Co., 1972, U.S.A., Pág. 110-101, 138-139.
[61] Cabanellas de Torres, Guillermo. Diccionario Jurídico Elemental, Editorial Heliasta S.R.L, Buenos Aires, Argentina, 1994. Pág. 115
[62] Mustapich, J. M., Tratado de Derecho Notarial, tomo I.
[63] Planiol y Ripert, Traite Pratique de Droit Civil Frangais, tomo VI, núm. 1458

rasgos que no sólo no expresan el nombre del firmante, sino que no tienen semejanza con los caracteres alfabéticos.

*Planiol y Ripert*, incurren en la misma falta de comprensión al decir que la firma indica el nombre de una persona, lo que no es del todo exacto, por las razones antes expuestas.

## 3.3 CLASES DE FIRMAS:

**a)** Firma Autógrafa.
**b)** Firma Mecánica.

### 3.3.1 LA FIRMA 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.[64]

En su aspecto jurídico, la firma autógrafa implica el hecho de tratarse de una inscripción manuscrita, realizada de una manera particular, hecha con el ánimo de obligarse al reconocimiento del escrito en que se estampe.

Algunas veces la firma la constituyen el nombre y los dos apellidos o alguno de éstos, manuscritos de una manera particular, o bien, de una o dos iniciales más un apellido, así como rasgos diversos; sin embargo, según otros, la firma puede estar constituida por los caracteres, signos o nombre que use o estampe determinada

[64] ACOSTA ROMERO, Miguel; OP. CIT.

persona, en un documento para obligarse a responder del contenido de ese documento, o para hacer constar que ha recibido alguna cosa.
En opinión de Planiol, no es necesariamente la reproducción de los nombres que la persona lleva según su estado civil; que sea la forma habitual de la cual la persona se sirva para firmar.[65] En gran parte de los países americanos y europeos se entiende como firma completa la que se integra con el nombre y apellido; en México, el uso mercantil entiende por media firma la sola inscripción de la rúbrica o inicial, y por firma completa la que comprende el nombre y apellidos o bien la totalidad de los rasgos que se utilizan como firma en los documentos.

No toda firma tiene efectos jurídicos, sin embargo, para el Derecho en general, se entiende que la colocación en un documento, en una obra de arte en un escrito de la palabra o palabras, o signos que utiliza su autor para identificarse, tienen el efecto jurídico respecto de las obras de arte, de identificarlas como hechas por el autor y respecto de los escritos, de identificar a la persona que los suscribe aun cuando el texto no haya sido escrito, en todo, ni en parte por esta.

El Derecho establece diversos efectos respecto de las categorías que como prueba puede establecer la firma en un documento. Carnelutti señala que en la suscripción actual se han fundado la manifestación del autor y la declaración de patronato, que originalmente eran distintos, sin embargo, en la actualidad se conjugan con el solo efecto de identificar a aquel que está suscribiendo un documento y es así que la firma establece la presunción de que el documento vale en cuanto está firmado y si no está firmado, no tiene alguna validez; criterio que ha sido tomado por la Suprema Corte de Justicia.

### 3.3.2 LA FIRMA MECÁNICA.

Es la que se realiza por medios mecánicos.

[65] Planiol, M., Traite Elémentaire de Droit Civil, tomo II, núm. 62.

Los medios mecánicos más utilizados, son los siguientes:

**1.** Facsímile.

**2.** Las máquinas de firma.

### 3.3.2.1 EL FACSÍMILE

Es la reproducción de la firma en sellos que pueden ser de goma o metálicos, y qué mediante su impregnación de tinta en cojines, receptores de éste, el sello puede ser estampado en cualquier escrito o documento.

La etimología, conforme al diccionario de la palabra facsímile, quiere decir lo siguiente:[66] imitación, semejanza, etcétera.

El sello de goma o metálico o de plástico, que contiene lo que podríamos calificar "de la copia en relieve de la firma autógrafa", se puede utilizar en forma manual o bien, por otros medios mecánicos para estamparla más rápidamente. El uso comercial y administrativo hace por ejemplo, que se utilice en los términos siguientes:

**a)** Para estampar el facsímile en las copias de la correspondencia, cuyo original va firmado, para evitar pérdidas de tiempo a los funcionarios que firman.

**b)** Para estamparla en la correspondencia de las empresas que por su volumen implique un gran número de cartas dirigidas a clientes, proveedores, etcétera, y que contenga generalmente datos informativos de diversa índole, en fin, qué por su volumen como ya se dijo, resulte muy difícil o laborioso la firma autógrafa.

[66] Facsímile. (Del latín Fac. Irnperat de faceré, hacer, y simple, semejante.) M. Exacta imitación de un escrito, dibujo, firma, etc. Ad." "Facsímil. M. Facsímile. Abad." Nueva Enciclopedia Sopeña. Diccionario ilustrado de la Lengua Española. Tomo II, p. 1044. Editorial Ramón Sopeña, S. A. Provenza 95, Barcelona, 1955

#### 3.3.2.2 LA MÁQUINA DE FIRMA.

En cierta época y en el uso comercial de Estados Unidos, hacia 1912, se inventó una máquina destinada a la múltiple reproducción de la firma autógrafa que, tal como la describe la Enciclopedia Espasa Calpe, resulta ser en realidad un pantógrafo, es decir, una máquina que con engranaje y palancas acciona una serie de plumas que siguen el trazo original y estampan en varios documentos a la vez la firma autógrafa, tal como la escribe la persona que la acciona.

Esta máquina parece ser poco práctica, porque el número de documentos que podría firmar es bastante limitado y el espacio que ocuparía sería muy grande. En El Salvador no se conoce ni se utiliza este tipo de máquinas.

La escritura a máquina o con linotipia no es autógrafa, aun cuando los respectivos teclados sean pulsados por el autor, ni lo es tampoco la que componga el autor utilizando tipos de imprenta. Esta distinción tiene importancia jurídica porque la escritura a mano contrariamente a lo que sucede con las mecanizadas, presenta particularidades y características propias de la persona que escribe, hasta el punto de que pericialmente se puede llegar a la identificación de una escritura o mejor dicho del autor de la misma aun cuando haya pretendido desfigurarla ya que los caracteres escritos ofrecen una fuerte personalidad con la que se pretende deducir de ellos las cualidades psíquicas de quien los ha trazado, a esto se encamina el arte que algunos consideran ciencia de la grafología.

## 3.4 CARACTERÍSTICAS DE LA FIRMA

De las anteriores definiciones se desprenden las siguientes características:

### 3.4.1 IDENTIFICATIVA:

Sirve para identificar quién es el autor del documento.

### 3.4.2 DECLARATIVA:

Significa la asunción del contenido del documento por el autor de la firma, sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

### 3.4.3 PROBATORIA:

Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal, en el acto de la propia firma.

## 3.5 ELEMENTOS DE LA FIRMA.

Al respecto es necesario distinguir entre:

### 3.5.1 ELEMENTOS FORMALES.

Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la misma:

#### 3.5.1.1 SIGNO PERSONAL.

La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

#### 3.5.1.2 EL ANIMUS SIGNANDI.

Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento.

### 3.5.2 ELEMENTOS FUNCIONALES.

Conociendo la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

### 3.5.2.1 IDENTIFICADORA.

La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones. La firma manuscrita expresa la identidad, aceptación y autoría del firmante.

### 3.5.2.2 AUTENTICACIÓN.

El autor del acto expresa su consentimiento y hace propio el mensaje.
Resumiendo, la función primordial de la firma no es entonces la identificación del firmante, sino la de ser el instrumento de su declaración de voluntad, que exige esa actuación personal del firmante en la que declara que aquello es un documento y no un proyecto o un borrador, que el documento está terminado y declara que el firmante asume como propias las manifestaciones, declaraciones o acuerdos que contiene

Algunos autores consideran que la firma, como exteriorización de la declaración de voluntad de una persona es imprescindible en los documentos comerciales, no es un mero requisito, la cual precisa de una actuación personal del firmante, una actuación física, corporal del firmante mismo, porque solo así puede ser instrumento de su declaración de voluntad.

En éste sentido, no estoy de acuerdo, ya que considero que si la firma es la exteriorización de la declaración de voluntad de una persona, ésta exteriorización puede hacerse por otro medio, como pudiera ser el electrónico siempre que la haga el firmante o legalmente se atribuya a él. Y aquí retomo lo comentado en párrafos anteriores sobre la función identificativa de la firma, pero ahora con el calificativo de electrónica, pues ésta sí requiere de identificación del autor para dar certeza de que es él y no un tercero quien declara su voluntad, de ahí el siguiente apartado “Firma Electrónica”

## 3.6 FIRMA ELECTRÓNICA

### 3.6.1 GENERALIDADES

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

### 3.6.2 CONCEPTO

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

Es aquél conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, contenido en un soporte magnético ya sea en un disquete, algún dispositivo externo o disco duro de una computadora y no de papel), que permite identificar a su autor, es decir que es el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcional mente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.[67]

[67] STROKE PAUL, "La Firma Electrónica" Editorial Cono Sur, España, pp. 17-18.

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

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

En otras palabras, podríamos definir a la Firma electrónica como el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o autores del documento que la recoge. La debilidad en cuanto al emisor y al receptor radica en la posible suplantación de la identidad de algunos de ellos, por parte de elementos ajenos al sistema.

Para evitar estos problemas, existen dos tipos de soluciones tecnológicas: el cifrado de los datos y la firma electrónica. Con el primero se puede transformar un texto claro en otro completamente ininteligible, que aun capturado sea prácticamente imposible de adivinar. Con la segunda, se consigue garantizar que quien envía los datos, es realmente quien dice ser y no otro, y que dichos datos no han sido manipulados en el camino.

## 3.7 ENCRIPTACIÓN O CIFRADO DE DATOS

### ANTECEDENTES

El origen de la criptografía data de el año 2000 AC., con los egipcios y sus jeroglíficos. Los jeroglíficos estaban compuestos de pictogramas complejos, donde sólo el significado completo podría ser interpretado por algunos.

El primer indicio de criptografía moderna fue usado por Julio César (100 AC. a 44 AC.), quien no confiaba en sus mensajeros cuando se comunicaba con los gobernadores y oficiales. Por esta razón, creó un sistema en donde los caracteres eran reemplazados por el tercer caracter siguiente del alfabeto romano. No solo los romanos, sino los árabes y los vikingos hicieron uso de sistemas de cifrado.

En la Grecia antigua, los militares utilizaban la criptografía, que aunque de manera rudimentaria, sus efectos eran los mismos: esconder un mensaje importante. Ellos utilizaron un sistema llamado *SCYTALE*, el cual se basaba en un báculo pequeño. En este instrumento enredaban un listón delgado, de tal manera que quedara forrado. Finalmente, sobre el báculo forrado por el listón, escribían el mensaje a ser enviado al ejército aliado.[68]

Posteriormente, este listón era desenrollado y en él quedaba escrito un mensaje indescifrable a simple vista, pudiendo enviarse este mensaje de manera "segura".

Cuando el listón era enrollado en un báculo con las mismas dimensiones, se podía entender el mensaje. De esta forma sólo los ejércitos amigos tenían una réplica exacta del instrumento para "encriptar" y "desencriptar" los mensajes importantes.

Gabriel de Lavinde hizo de la criptografía una ciencia más formal cuando publicó su primer manual sobre Criptología en 1379.

[68] STROKE PAUL, "La Firma Electrónica" Editorial Cono Sur, España, pp. 23-24

Samuel Morse. El Código Morse, desarrollado en 1832, aunque no es propiamente un código como los otros, es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos. En tiempos modernos, la criptografía se ha convertido en una compleja batalla entre los mejores matemáticos del mundo y de los ingenieros en sistemas computacionales. La habilidad de poder almacenar de manera segura y de transferir la información ha dado un factor de éxito en la guerra y en los negocios.

Dado a que los gobiernos no desean que ciertas entidades entren y salgan de sus países para tener acceso a recibir o enviar información que puede comprometer y ser de interés nacional, la criptografía ha sido restringida en muchos países, desde la limitación en el uso, la exportación o la distribución de software de conceptos matemáticos que pueden ser usados para desarrollar sistemas criptográficos.

De cualquier manera, el Internet ha permitido que todas estas herramientas sean distribuidas, así como las tecnologías y técnicas de criptografía, de tal manera, que al día de hoy, la mayoría de los sistemas criptográficos avanzados están en el dominio público.

La criptografía incluye técnicas como esconder texto en imágenes y otras formas de esconder información almacenada o en tránsito.

Simplificando el concepto, hoy en día la criptografía se asocia más a convertir texto sencillo a texto cifrado y viceversa. La Criptografía se ocupa de dar solución a los problemas de identificación, autenticación y privacidad de la información en los sistemas informáticos. Debido a la naturaleza de un medio no físico, no resultan útiles los métodos tradicionales de sellar o firmar documentos, con propósitos comerciales o legales.

**ETIMOLOGÍA**

**Criptografía**[69]

I. Del griego kryptos = oculto + graphe = escritura.

1. (sustantivo femenino). Escritura en clave.

**Críptolalia**

I. Del griego krypto = yo oculto + ¡aleo = yo hablo.

1. (sustantivo femenino). Alteración de la lengua hablada con el fin de que no pueda ser comprendida si no se conoce la clave.

Escritura utilizada para proteger los mensajes de alteraciones y modificaciones. Aunque el término se ha utilizado desde el siglo XVII, el concepto se ha utilizado desde tiempos inmemorables. Los primeros intentos de criptografía fueron basados en el habla, mas que en la escritura: críptolalia. Aquellos que hablaban más de una lengua aprovechaban esto delante de gente que no los entendía para intercambiar información que buscaban mantener en secreto.

El primer uso que tuvo la criptografía fue militar[70], aunque la necesidad de proteger un secreto, se incrementó a medida que aumentaba el valor de cierta información. Durante el último siglo, hubo desarrollos en técnicas criptográficas que evolucionaron de manuales a electrónicas, pasando por las mecánicas.

**CONCEPTO**

Criptografía es la ciencia de mantener en secreto los mensajes. El texto original, o texto puro es convertido en un equivalente en código, llamado críptotexto (ciphertexf) via un algoritmo de encripción. El criptotexto es decodificado (decriptado) al momento de su recepción y vuelve a su forma de texto original.

[69] Rubio Velásquez, Rodríguez Sau, Muñoz Muñoz., La Firma Electrónica, Aspectos Legales y Técnicos, Edición Barcelona, 2004, Pág. 179.
[70] Ídem

También la criptografía es definida como: “es la ciencia que se ocupa de transformar mensajes en forma aparentemente ininteligibles y devolverlos a su forma original”.[71]

La criptología se define como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Abarca por tanto a la Criptografía (datos, texto, e imágenes), Criptofonía (voz) y al Criptoanalisis (ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto claro original, pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave).

Cifrar por tanto, consiste en transformar una información (texto claro) en otra ininteligible (texto cifrado o criptó), según un procedimiento y usando una clave determinada, pretendiendo que sólo quién conozca dicho procedimiento y clave pueda acceder a la información original. La operación inversa se llamara lógicamente descifrar. La seguridad de un fuerte sistema criptográfico, reside en el secreto de la llave más que en el secreto del algoritmo. En teoría, cualquier método criptográfico puede "romperse" (descifrarse) intentando todas las posibles llaves (claves o combinaciones) en secuencia.

En algunos casos en los que la autenticación de la persona resulta crítica, como en el pago con tarjeta de crédito, se puede exigir incluso que estampe una firma, que será comparada con la que aparece en la tarjeta y sobre su documento de identificación. En el mundo físico se produce la verificación de la identidad de la persona comparando la fotografía del documento con su propia fisionomía y en casos especialmente delicados, incluso, comparando su firma manuscrita con la estampada en el documento acreditativo que porta. En otras situaciones, no se

[71] Martínez Nadal, a., Comercio electrónico, Firma Digital y Autoridades de Certificación, 3ª Edición, Civitas, Madrid, 2001 Pág. 45.

requiere la credencial de elector o pasaporte, pero sí la firma, para que el documento goce de la validez legal (cheques, cartas, etc.), ya que ésta vincula al signatario con el documento por él firmado.

El fundamento de las firmas electrónicas es la criptografía, disciplina matemática que no sólo se encarga del cifrado de textos para lograr su confidencialidad, protegiéndolos de ojos indiscretos, sino que también proporciona mecanismos para asegurar la integridad de los datos y la identidad de los participantes en una transacción. El cifrado consiste en transformar un texto en claro (inteligible por todos) mediante un algoritmo en un texto cifrado, gracias a una información secreta o clave de cifrado, que resulta ininteligible para todos excepto para el legítimo destinatario del mismo. Se distinguen dos métodos generales de cifrado: Cifrado de Llave Privada o Simétrica y Cifrado de Llave Pública o Asimétrica.

Es así que el objetivo de la criptografía es el de proporcionar comunicaciones seguras (y secretas) sobre canales inseguros. Ahora bien, la criptografía no es sinónimo de seguridad. No es más que una herramienta que es utilizada de forma integrada por mecanismos de complejidad variable para proporcionar no solamente servicios de seguridad, sino también de confidencialidad.

### 3.7.1 CLASES DE CRIPTOGRAFÍA

#### 3.7.1.1 CIFRADO DE LLAVE PRIVADA O SIMÉTRICA

Aquella en la que la llave de encripción es la misma de desencripción. Por tanto estamos ante un criptosistema Simétrico o de Clave Secreta[72] cuando las claves para cifrar y descifrar son idénticas, o fácilmente calculables una a partir de la otra.. Esto quiere decir que si utilizamos un criptosistema de clave secreta o simétrico, necesariamente las dos partes que se transmiten información tienen que compartir el secreto de la clave, puesto que tanto para encriptar como para

[72] Nash, a.- Duane,w.- Joseph,c-Brink,D., PKI Infraestructura de las claves publicas, McGraw Hill, Bogota, Colombia,2002, pag 21y siguientes.

desencriptar se necesita una misma clave u otra diferente pero deducible fácilmente de la otra. Entre estos sistemas se encuentran: "DES, RC2, RC4, IDEA, SkipJack etc.". La peculiaridad de estos sistemas de encriptación es que son rápidos en aplicarse sobre la información.[73]

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos.

Ésta es la opción utilizada para cifrar el cuerpo de los mensajes en el correo electrónico o los datos intercambiados en las comunicaciones digitales. Es decir que se trata del mecanismo clásico por el cual se utilizan técnicas que usan una clave K que es conocida por el remitente de los mensajes y por el receptor, y con la que cifran y descifran respectivamente el mensaje. Para mantener la seguridad del cifrado, deben mantener esta clave en secreto. Las ventaja del uso de estas claves es la existencia de algoritmos muy rápidos y eficientes para su cálculo.

El principal inconveniente estriba en la necesidad de que todas las partes conozcan K, lo que lleva a problemas en la distribución de las claves. Esta debilidad ha hecho que sea poco utilizada en los mecanismos desarrollados hasta el momento para permitir el pago, a no ser que vaya combinada con otro tipo de técnicas.

El sistema de cifrado más extendido es *Data Encryption Standard (DES),* desarrollado por IBM y adoptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977. Una mejora de este sistema de cifrado de clave simétrica es IDEA.

[73] Ídem 46-49

#### 3.7.1.1.1 CARACTERÍSTICAS PRINCIPALES DE LAS LLAVES PRIVADAS

1. Solo existe una llave privada por individuo

2. Para uso único del propietario

3. Es secreta

4. Se usa para desencriptar información y generar firmas

**DESVENTAJAS DE LA CIFRADO TRADICIONAL**

- Quien envía y quien recibe un mensaje necesitan compartir la misma llave, lo que significa que cada uno debe confiar en el otro para que no comprometa la información que exclusivamente la conocen ellos dos.

- Quien envía y quien recibe tienen un problema de distribución.

- No es posible comunicar de manera segura la "llave secreta" ambas partes que la necesitan, sin irse "fuera de línea" (usar un canal de comunicación distinto, como el correo tradicional).

### 3.7.1.1.3 FUNCIONAMIENTO CRIPTOGRAFÍA DE CLAVE SIMÉTRICA.

Se emplea una sola clave para cifrar y descifrar el mensaje.
**Proceso:**

Ana ha escrito un mensaje para Bernardo pero quiere asegurarse de que nadie más que él lo lee. Por esta razón ha decidido cifrarlo con una clave. Para que Bernardo pueda descifrar el mensaje, Ana deberá comunicarle dicha clave.



Bernardo recibe el mensaje y la clave y realiza el descifrado.


El **beneficio** más importante de las criptografía de clave simétrica es su velocidad lo cual hace que éste tipo de algoritmos sean los más apropiados para el cifrado de grandes cantidades de datos.

El **problema** que presenta la criptografía de clave simétrica es la necesidad de distribuir la clave que se emplea para el cifrado por lo que si alguien consigue hacerse tanto con el mensaje como con la clave utilizada, podrá descifrar el mensaje.

Por esta razón se plantea el uso de un sistema criptográfico basado en claves asimétricas, como veremos a continuación.

### 3.7.1.2 CIFRADO DE LLAVE PÚBLICA O ASIMÉTRICA

Cada persona tiene un par de llaves, una pública[74] que todos conocen, y la otra privada que sólo su propietario conoce. En cambio, si A y B usan la criptografía asimétrica, ambos tienen un juego de llaves, una pública que cualquier persona puede conocer, y otra privada que sólo su dueño conoce. En este caso, A envía un mensaje a B. Llave Pública de B y Llave Privada de B. A usa la llave pública de B para encriptar el mensaje que le envía. B usa su llave privada para desencriptar el mensaje que le envió A, y verifica la identidad de A con su llave publica.

La Firma Electrónica Avanzada, para cumplir con los requisitos de autenticación, fiabilidad e inalterabilidad requiere de métodos de encriptación, como el llamado asimétrico o de clave pública. Éste método consiste en establecer un par de claves asociadas a un sujeto, una pública, conocida por todos los sujetos intervinientes en el sector, y otra privada, sólo conocida por el sujeto en cuestión, aunque la norma de análisis no habla del sistema de encriptación, si menciona el uso de medios electrónicos de identificación y contraseñas, en mensajes de datos, esto no es otra cosa que una clave privada que nos va permitir la perfecta identificación de su emisor objeto de la autenticidad de la Firma Electrónica a través de mensajes de datos.[75]

De esta forma, cuando quiera establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo, en el precepto no era necesario establecer la forma técnica de hacerlo, solo era necesario dar a conocer el hecho de un sistema de identificación a través de claves o contraseñas para poder emplearla al momento de la generación de la información.
Si A y B desean autenticar un documento, el proceso es al revés. A quiere enviar un documento a B, para que éste lo autentifique, es decir, para que B pueda

[74] Nash, a.- Duane,w.- Joseph,c-Brink,D., op. Cit, Pág. 28 y siguientes.
[75] PEÑALOZA EMILIO “La protección de datos personales” Editorial Díaz de Santos, España, pp. 114.

comprobar que dicho documento sólo puede provenir de A. Este proceso se conoce como firma electrónica avanzada. Cualquier persona que conozca la llave pública de A (todos la conocen), puede desencriptar el documento con esa llave. Así es como existe una Llave Privada de A y una Llave Pública de A. Es así que A encripta el documento con su llave privada y lo envía a B. Por lo que B desencripta el documento con la llave pública de A.

Es decir, que estas claves públicas existen cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto con ella cifrado. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas electrónicas avanzadas

En general, el cifrado asimétrico se emplea para cifrar las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través de la Red junto con el documento cifrado, para que en recepción éste pueda ser descifrado. La clave de sesión se cifra con la clave pública del destinatario del mensaje, que aparecerá normalmente en una libreta de claves públicas. En principio, bastaría con cifrar un documento con la clave privada para obtener una firma electrónica avanzada segura, puesto que nadie excepto el poseedor de la clave privada puede hacerlo. Posteriormente, cualquier persona podría descifrarlo con su clave pública, demostrándose así la identidad del firmante.[76]

[76] Ídem

En la práctica, debido a que los algoritmos de clave pública requieren mucho tiempo para cifrar documentos largos, los protocolos de firma electrónica avanzada se implementan junto con funciones unidireccionales de resumen (funciones hash), de manera que en vez de firmar un documento, se firma un resumen del mismo. Es decir que los sistemas asimétricos de cifrado, siendo los más populares los de clave pública. Estas técnicas se basan en la existencia de parejas de claves, una secreta o privada (Ks), conocida únicamente por su propietario, y una pública (Kp), libremente distribuida por su propietario en toda la red. El conocimiento de una de las claves no permite averiguar la otra. Un mensaje es cifrado con una de las claves y descifrado con la otra.

Uno de los primeros esquemas de clave pública, fue desarrollado por R. Rivest, A. Shamir y L. Adleman. El esquema Rivest-Shamir-Adleman (RSA) ha sido desde la fecha de su publicación, el único sistema ampliamente aceptado para la implementación de encriptación mediante clave pública. El principal inconveniente de este sistema era la existencia de una patente sobre este algoritmo, lo cual dificulta su uso fuera de los Estados Unidos, si no se ha obtenido la correspondiente licencia de exportación; la gran ventaja es que ha pasado el tiempo y actualmente éste sistema es del dominio público.

Gracias a las firmas electrónicas, los ciudadanos pueden realizar transacciones de comercio electrónico verdaderamente seguras, y relacionarse con la máxima eficacia jurídica. En la vida cotidiana se presentan muchas situaciones en las que los ciudadanos deben acreditar fehacientemente su identidad, por ejemplo, a la hora de pagar las compras con una tarjeta de crédito en un establecimiento comercial, para votar en los colegios electorales, con el fin de identificarse en el mostrador de una empresa, al firmar documentos notariales o una sencilla carta enviada a un amigo, etc.

En estos casos, la identificación se realiza fundamentalmente mediante la presentación de documentos acreditativos como la credencial de elector, el pasaporte o el carnet de conducir, que contienen una serie de datos significativos vinculados al individuo que los presenta, como:

- Nombre del titular del documento.
- Número de serie que identifica el documento.
- Período de validez: fecha de expedición y de caducidad del documento, más allá de cuyos límites éste pierde validez.
- Fotografía del titular.
- Firma manuscrita del titular.
- Otros datos demográficos, como sexo, dirección, etc.

Los primeros sistemas criptográficos utilizaban combinaciones más o menos complejas de la técnica de rotación de los caracteres de un mensaje. La seguridad de este tipo de sistemas se basaba en mantener secreto el algoritmo usado, y son fácilmente descifrables usando medios estadísticos. En la actualidad sólo son utilizados por aficionados.

En medios profesionales, se usan criptosistemas. Se trata de funciones matemáticas parametrizadas en las que los datos de entrada no se pueden obtener a partir de los de salida, salvo en plazos tan largos que cualquier información obtenida ya no tiene valor. La seguridad se basa ahora, no en mantener secreto el algoritmo, que generalmente es público, sino los parámetros (claves) del mismo.

Firmar electrónica un documento consiste en pasar un determinado algoritmo sobre el texto que se desea cifrar, basándose en la clave privada del signatario electrónico. Cuando el texto debe transmitirse firmado, el algoritmo recorre todos

sus datos electrónicos , junto a la clave privada, obtiene un valor ("hash"), que es la llamada firma digital.

En la transmisión, se envía por una parte el documento cifrado, y por otra el hash. Cuando el receptor recibe ambos documentos, debe actuar bajo las siguientes pautas:

- Descifra el texto del destinatario con la clave pública.

- Con este texto calcula el hash.

- Si el hash calculado y el enviado coinciden, eso significa que el documento que ha llegado lo envía quien dice ser (ha sido descifrado con su clave "contraria") y que además no ha sido alterado por el camino, pues de lo contrario los dos hash no coincidirían.

#### 3.7.1.2.1 CARACTERÍSTICAS PRINCIPALES DE LAS LLAVES PÚBLICAS

**1.** El usuario solo puede tener una llave pública.

**2.** Es puesta a disposición de todos los usuarios.

**3.** Se usa para encriptar información y generar firmas electrónicas avanzadas.

#### 3.7.1.2.2 VENTAJAS DE LA CRIPTOGRAFÍA ASIMÉTRICA

- **Imposibilidad de suplantación**: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, control

biométrico, una tarjeta inteligente, etc.) Asegura, además, la imposibilidad de su suplantación por otro individuo.

- **Integridad**: permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados. Consiste en conocer que un mensaje de datos no ha sido alterado ni manipulado durante el envío. La firma electrónica avanzada tienen un sistema que garantiza la integridad del mensaje, puesto que si el mensaje enviado hubiese sido modificado después de haber sido cifrado, esta transformación del mensaje constará al destinatario, puesto que el resumen no resultará coincidente con el original enviado si el mensaje de descifra con la clave pública correspondiente. Si no ha sido modificado, coincidirá plenamente con el original firmado por el emisor.

Esta es una diferencia que contrapone a la firma electrónica avanzada frente a la firma electrónica en general, puesto que en esta segunda, no existen tantas garantías de integridad del mensaje de datos como en la firma electrónica segura.

En la Ley Modelo de la UNCITRAL sobre las Firmas Electrónicas elaborado, en el apartado primero del artículo 5, establece una presunción de integridad: "Si el presunto firmante ha utilizado un procedimiento de seguridad que puede brindar la prueba fiable de que un mensaje de datos o una firma electrónica segura refrendada consignada en él no ha sido modificado desde el momento en que el procedimiento de seguridad se aplicó al mensaje de datos o a la firma, entonces se presumirá en ausencia de toda prueba de lo contrario, que el mensaje de datos o la firma no han sido modificados."

- **No repudio**: ofrece seguridad inquebrantable de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma electrónica adjunta a los datos, debido a la imposibilidad de ser falsificada, testimonia que él, y solamente él, pudo haberlo firmado.

- **Auditabilidad**: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático, cuyo acceso se realiza mediante la presentación de certificados, especialmente cuando se incorpora el estampillado de tiempo, que añade de forma totalmente fiable la fecha y hora a las acciones realizadas por el usuario.

- **Privacidad**: asegurar que la comunicación solo se da entre aquellos autorizados.

- **No rehusabilidad**: Prevenir que la información no pueda duplicarse.

Es por estas características, que la firma electrónica avanzada, es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Una persona, llamada signatario, firma documentos mediante un dispositivo de creación de firma y unos datos de creación de firma; el destinatario del documento firmado debe verificar, mediante un dispositivo de verificación de firma y un certificado digital, la firma del signatario. De este modo, el signatario es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa. Se entiende

que su actuación se refiere al acto de firmar un documento, dentro del marco, como veremos, de una política de firma electrónica. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica y los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

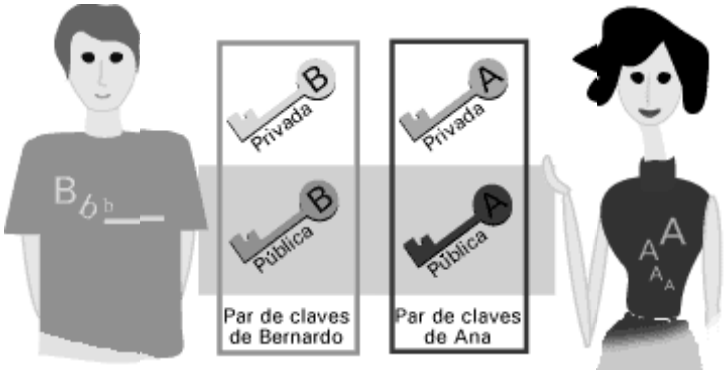
En resumen, el sistema de encriptación asimétrica y la firma electrónica avanzada constituyen el primer gran paso hacia la seguridad en las transacciones comerciales por vía electrónica, dado que el par de claves (pública y privada) de cada usuario de la red electrónica ha de ser diferente (es lo que se denomina carácter único de la clave), el procedimiento de emisión o generación de claves debe estar sujeta a auditorias de calidad, con el fin de mantener la unicidad.

Los anteriores datos de creación de firma electrónica, deben ser empleados por un dispositivo de creación de firma, que posee el signatario: para que la firma electrónica tenga un valor superior, veremos que el dispositivo de creación de firma, debe cumplir determinados requisitos (en ese caso se denomina dispositivo seguro de creación de firma); igualmente, el destinatario de un mensaje firmado, debe disponer de un dispositivo de verificación de firma.

### 3.7.1.2.3 FUNCIONAMIENTO CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA.

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:
**Clave privada**: será custodiada por su propietario y no se dará a conocer a ningún otro.
**Clave pública**: será conocida por todos los usuarios.
Esta pareja de claves es complementaria: **lo que cifra una SÓLO lo puede descifrar la otra y viceversa**. Estas claves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra.
**Proceso:**

Ana y Bernardo tienen sus pares de claves respectivas: una clave privada que sólo ha de conocer el propietario de la misma y una clave pública que está disponible para todos los usuarios del sistema.




Ana escribe un mensaje a Bernardo y quiere que sólo él pueda leerlo. Por esta razón lo cifra con la clave pública de Bernardo, accesible a todos los usuarios.


Se produce el envío del mensaje cifrado no siendo necesario el envío de la clave.


Sólo Bernardo puede descifrar el mensaje enviado por Ana ya que sólo él conoce la clave privada correspondiente.


El **beneficio** obtenido consiste en la supresión de la necesidad del envío de la clave, siendo por lo tanto un sistema más seguro.
El **inconveniente** es la lentitud de la operación. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica.

## Criptografía de Clave Asimétrica. Cifrado de Clave Pública.

El uso de claves asimétricas ralentiza el proceso de cifrado. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica. A continuación veremos cómo se produce el cifrado de un mensaje, mediante el cual obtenemos plena garantía de confidencialidad.

## Proceso:

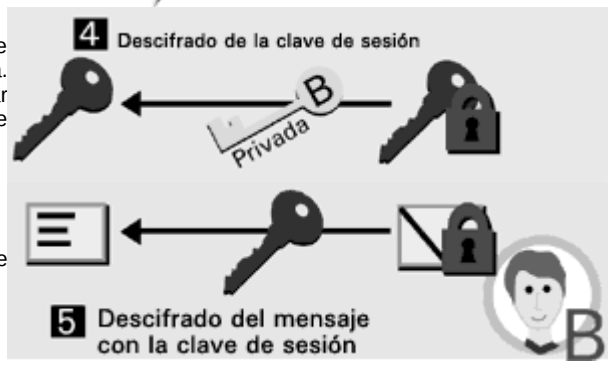
Ana y Bernardo tienen sus pares de claves respectivas.

Ana escribe un mensaje a Bernardo. Lo cifra con el sistema de criptografía de clave simétrica. La clave que utiliza se llama clave de sesión y se genera aleatoriamente.

Para enviar la clave de sesión de forma segura, esta se cifra con la clave pública de Bernardo, utilizando por lo tanto criptografía de clave asimétrica..


Bernardo recibe el mensaje cifrado con la clave de sesión y esta misma cifrada con su clave pública. Para realizar el proceso inverso, en primer lugar utiliza su clave privada para descifrar la clave de sesión.

Una vez ha obtenido la clave de sesión, ya puede descifrar el mensaje.




Con este sistema conseguimos:

**Confidencialidad**: sólo podrá leer el mensaje el destinatario del mismo.

**Integridad**: el mensaje no podrá ser modificado.

## 3.7.2 CARACTERÍSTICAS DE UN SISTEMA SEGURO

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

**CARACTERÍSTICAS DE UN SISTEMA SEGURO**

El comercio electrónico empezó a ser seguro a mediados de 1990, actualmente avanzados sistemas de seguridad ofrecidos por Internet, pueden asegurar el éxito de todas las transacciones económicas que se llevan a cabo en este medio, con el fin de que exista una celebración válida de negocios jurídicos que impliquen la viabilidad de expresar la voluntad de una persona y con ello la posibilidad de celebrar contratos válidos y exigibles.

Existen también riesgos derivados de los problemas inherentes a los mismos sistemas electrónicos a través de los que se desarrolla en una red abierta e insegura como Internet.

Los riesgos más importantes derivados de un intercambio de información a través de Internet son:

- Que el autor y fuente del mensaje haya sido suplantado, es el problema de la autoría de los mensajes electrónicos.

- Que el mensaje sea alterado, de forma accidental o intencional durante la transmisión o incluso una vez recibido, es el problema de la integridad de los mensajes electrónicos.

- Que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido, es el problema del repudio de los mensajes electrónicos.

- Que el contenido del mensaje sea leído por una persona no autorizada, es el problema de la confidencialidad de los mensajes electrónicos.

En esta transición de un sistema comercial basado en el papel a un sistema de comercio electrónico se hace necesario que la sustitución del papel y de las firmas escritas por sus equivalentes electrónicos pueda generar la misma confianza y ofrecer seguridad jurídica a los usuarios. Por lo tanto, para minimizar los riegos derivados del intercambio de información a través de Internet se utiliza la firma digital la cual proporciona una amplia gama de servicios de seguridad al cumplir con las siguientes características:

#### 3.7.2.1 AUTENTICIDAD

La autenticidad se preocupa por la fuente o el origen de una comunicación. ¿Quién mandó el mensaje? ¿Es genuino o una falsificación?

Al igual que la firma manuscrita se presume que ésta pertenece a la persona que la estampa con su puño y letra, la firma electrónica no es ajena a ésta manera de firmar, ya que expresa la autoría de la declaración de voluntad del signatario y que pertenece exclusivamente a la persona que consta como titular del certificado.

A ésta característica de la electrónica avanzada se le conoce como autenticidad, la cual consiste en que: "el mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema."[77] Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message Autentication Code).

Es decir que la autenticación permite identificar y sin equivocaciones quien es el signatario, ya que el hecho de que la firma ha sido creada por él, mediante medios que mantiene bajo su propio control, como por ejemplo, contraseñas, tarjetas inteligentes, etc., aseguran la imposibilidad de su suplantación, aspecto de especial relevancia, ya que el medio utilizado para la difusión de los mensajes es el Internet, el cual por si solo no brinda la confianza y seguridad en los usuarios como la proporciona el uso de la firma electrónica.

#### 3.7.2.2 CONFIDENCIALIDAD

El comercio se desarrolla por medios electrónicos, a través de una red abierta como Internet, la cual no proporciona seguridad a los usuarios, y se hace necesario garantizar la confidencialidad, ya que existen empresas que utilizan Internet para el envío y recepción de información sumamente importante y que no

[77] www.scba.gov/fdweb.swf

puede ser interceptada por otra empresa, ya que esto implicaría un peligro para su seguridad.

Por confidencialidad entenderemos, “el mayor o menor grado de secreto al que la persona quiere someter a un dato o una información; lo cual va a depender de los intereses particulares o personales del poseedor del dato e independientemente de cuestiones puramente jurídicas o de relaciones contractuales.”[78]

La aplicación de las tecnologías de firma digital hace posible, que esta característica de confidencialidad, sea cubierta ya que un mensaje cifrado con firma digital “protege los datos de revelaciones o accesos de personas no autorizadas.”[79]

La obtención de confidencialidad en la transmisión de datos, implica el uso de tecnologías basadas en la criptografía, como el cifrado, aspecto que desarrollaremos mas adelante.

#### 3.7.2.3 INTEGRIDAD

La integridad se preocupa por la certeza y lo completo de la comunicación. ¿Es el documento el recipiente recibió el mismo como el documento que el emisor mandó? ¿Es completo? ¿Ha sido alterado el documento o en transmisión o almacenamiento?

La integridad es una de las características con las cuales se le da plena validez jurídica al documento electrónico, y es por esto que se confía en la firma digital, ya que “asegura la información de manera que ésta, no pueda ser modificada o alterada, ya sea intencionalmente o accidentalmente. El mensaje debe llegar a su

[78] Escuela Judicial Concejo General del Poder Judicial. Problemática jurídica en torno al fenómeno de Internet. Cuadernos de Derecho Judicial. Imprime: LERKO PRINT, S.A. 2000. Pág. 152
[79] Op. Cit. Martínez Nadal. Pág. 38.

destino sin alteraciones en su contenido o en el orden de la recepción de las unidades."[80]

Doctrinariamente, muchos autores coinciden en la relevancia de ésta característica, principalmente porque se trata de datos firmados y enviados entre personas que en ningún momento llegan a tener un contacto directo entre ellos, y gracias a la característica de la integridad que tiene la firma digital, se presume que el mensaje recibido es el que se ha enviado.

Es por lo anteriormente dicho, que la integridad permite que sea detectada cualquier modificación por pequeña que sea, de los datos firmados, proporcionando así, una garantía ante alteraciones accidentales o provocadas, durante el manejo de documentos o datos firmados.

#### 3.7.2.4 NO REPUDIO

Cuando se firma un documento, lo que se hace es manifestar que está acorde con el contenido del mismo, por ende cuando un documento electrónico se encuentra firmado por medio de firma digital, se deduce que el autor del mensaje que consta en el certificado, debidamente expedido, está manifestando que su voluntad es la consignada en dicho documento y por lo tanto no puede negarse a los efectos que del mismo derivan.

La figura del no repudio puede por tanto, ser definida como "una de las características resultantes de los contratos y documentos electrónicos, la cual protege a las partes de la negación de que dicha comunicación haya ocurrido, es decir que protege al receptor del documento de la negación del emisor de haberla enviado."[81]

[80] Polanco Villalobos, José Antonio y otros, La regulación sobre comercio electrónico en el ordenamiento jurídico salvadoreño, Tesis, Universidad José Simeón Cañas, 2001. Pág. 45.
[81] Op. Cit. Pág 22

Esta característica, es más fuerte que las anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje. A pesar de que no se puede conseguir el no repudio sin la autenticación y la integridad de los datos, el no repudio consiste en algo más, ya que es la capacidad de probar a un tercero que una determinada transmisión de información ha sido originada, admitida y enviada a determinada persona.

En el Derecho Norteamericano, el no repudio es el principio general del derecho probatorio, porque permite evadir la negativa tanto de haber recibido como de haber enviado el mensaje.

# CAPITULO IV

## 4.1 AUTORIDAD CERTIFICADORA

En el mercado electrónico, al mismo tiempo que ofrece más oportunidades, conlleva en sí, un gran número de procesos y sistemas, así como la necesidad de una mayor seguridad lógica en lo que se transmite a través de las redes públicas.

Las Autoridades Certificadoras del mercado electrónico, deben actuar como autoridades intermediarias, que certifiquen la identidad y solvencia de sus inscriptos, sus referencias financieras, sus capacidades para el comercio internacional, etc.; todo ello para justificar la confianza mínima necesaria entre las partes para poder realizar transacciones provechosas.

La forma más efectiva y aceptada hoy en día para realizar transacciones en el comercio electrónico entre proveedores y clientes que no han tenido una relación previa, es a través de clubes, mercados o market places de comercio electrónico. En tales casos, las empresas y clientes se limitan a comprar dentro de un mismo mercado que está centrado en ciertos sectores, regiones o grupos de interés. Mediante la asociación mutua a un mercado, tanto el comprador como el vendedor, confían en el gestor del mismo que, a través de una Autoridad de Certificación, asegura que cada parte es quién dice ser y cuenta con capacidad suficiente para actuar como agente de pleno derecho.

Cuando una parte contratante desea verificar la firma electrónica generada por la otra parte, la parte verificadora necesita una copia de la clave pública de la parte firmante y necesita tener la certeza de la correspondencia entre la clave pública y privada y que estas corresponden a una persona determinada.

Este problema se resuelve con los certificados de clave pública emitidos por una autoridad de certificación que actúa como tercera parte de confianza de la parte firmante y de la parte verificadora.

**4.2 CONCEPTOS**

Es la entidad que genera y revoca los certificados para un conjunto de usuarios y es responsable de su autenticidad. Sus funciones se pueden resumir en:

1. Generación de certificados al garantizar su identidad por medio de una firma Electrónica.

2. Agendar fechas de expiración de certificados y

3. Revocar los certificados.

Una característica fundamental de la Autoridad Certificadora, es que sea un ente de alta confianza para la comunidad.

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

La terminología para referirse a las terceras partes de confianza es muy variada, desde la expresión autoridad, proveedor de servicios, prestador de servicios de certificación, entidad certificadora o simplemente certificador.

Las Autoridades Certificadoras son una pieza fundamental en el desarrollo del Comercio Electrónico, pues son los que brindan certeza sobre el autor y contenido de un mensaje de datos, y por lo mismo, de ellas depende el desarrollo de este tipo de canales de comunicación dentro de un marco de seguridad jurídica esencial para la proliferación del comercio por esta vía.

En nuestro caso, adoptamos la expresión de Autoridad Certificadora por su apariencia neutral.

Existe una amplia gama de definiciones de autoridad de certificación, para referirnos a ellas retomamos a algunos autores: *"La Autoridad Certificadora es un organismo dedicado a la emisión de certificados que contiene información sobre algún hecho o circunstancia del sujeto del certificado, en los casos de los certificados de clave pública, son certificados que vinculan un par de claves con una persona determinada de forma segura, cubriendo así la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas."*[82]

Otra definición de autoridad de certificación es:*"La persona física o jurídica, pública o privada, que expide, renueva y revoca certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica, como la validación de certificados."*[83]

Se puede afirmar que, la criptografía necesita de una tercera parte de confianza, es decir, una entidad certificadora que debe realizar la vinculación de una persona debidamente identificada con un par de claves determinadas y para ello necesita de una regulación que la controle y determine su responsabilidad, ya que para asociar un par de claves con un probable firmante, una entidad de certificación emite un certificado que ligue una clave pública con el sujeto del certificado, y confirma que el probable firmante identificado en el certificado tiene la correspondiente clave privada.

[82] Op. Cit. Martínez Nadal, "Comercio electrónico..." Pág 149
[83] www.hfernandezdelpech.com.ar/leyes/trab/firma%20digital.deusto%202002.htlm

## 4.3 FUNCIONES DE LAS AUTORIDAD CERTIFICADORA

Las funciones de una Autoridad de Certificación deben ser, entre otras, las siguientes:

1. Generación y Registro de claves.
2. Identificación de Peticionarios de Certificados.
3. Emisión de certificado.
4. Almacenamiento en la AC de su clave privada (si así lo autoriza el usuario).
5. Mantenimiento de las claves vigentes y revocadas.
6. Servicios de directorio.

### 4.3.1 GENERACIÓN Y REGISTRO DE CLAVES

Cualquiera que desee firmar electrónicamente un mensaje o recibir envíos cifrados y/o firmarlos, debe poseer un par de claves dentro de algún criptosistema de clave pública.

Los agentes pueden tener más de un par de claves: uno para el trabajo, otro con efectos administrativos, otro para uso personal, etc. Es más, otras autoridades de la red como son las estaciones de trabajo, los servidores, las impresoras, etc., también pueden (y deben) tener sus pares de claves; de la misma forma que lo harán personas jurídicas e instituciones como pueden ser los departamentos de las empresas, la secretaría de una universidad, la recepción de un hotel, etc.

Dado que la identidad de cada agente se basa en el secreto de una de las claves, la privada, cada usuario deberá generar por sus propios medios sus pares de claves. También puede ser que las organizaciones opten por instalar un servidor para la generación de las claves de todos sus empleados que lo soliciten, pero en ese caso debe tenerse muy en cuenta que el mantenimiento del sigilo por parte del generador debe ser una cualidad probada y auditable.

En cualquier caso, las claves privadas nunca deben viajar por la red y habrán de ser distribuidas a través de canales no telemáticos de seguridad y confidencialidad probadas. Por ello, siempre que se pueda, lo mejor es que cada nodo de la red sea capaz de generar localmente sus claves con lo que elimina la necesidad de su distribución.

Una vez, generada las claves, el usuario debe “registrar” su clave pública en una Autoridad de Certificación aceptada dentro del escenario en el cual pretende moverse. Para la inscripción sólo tiene que enviar su clave pública y, muy posiblemente, algún que otro documento digital de solicitud firmado condicha clave.

Al tratarse de documentos públicos, esta transmisión se puede hacer a través de la red sin menoscabo alguno de su integridad. Para completar el proceso de inscripción, el solicitante deberá:
Bien enviar otro Certificado Digital de Identidad expedido por alguna otra Autoridad de Certificación aceptada, o bien;

Deberá enviar un documento físico válido dentro de los procedimientos administrativos habituales en el que asume la responsabilidad del compromiso indicado en la solicitud digital que ha enviado. Satisfechas las condiciones marcadas por la Autoridad de Certificación en su documento público de Política de Emisión de Certificados incluida en su Política de Seguridad, esta autoridad devuelve al solicitante un certificado digital que atestigua la validez de su clave pública para actuar dentro del sistema.

Los sistemas de autenticación basados en claves simétricas y secretas, como es el caso de “Kerberos”, no permiten la generación local de claves sino que ésta es función del servidor central que constituye la Autoridad de Certificación.

### 4.3.2 IDENTIFICACIÓN DE PETICIONARIOS DE CERTIFICADOS

La emisión de Certificados de Identidad Personal exigen el reconocimiento previo de todos aquellos elementos característicos y únicos que son propios del solicitante; a estos caracteres se les denomina “identificadores intrínsecos” (fotografía, firma manuscrita, huellas dactilares, timbre de voz, fondo de ojo, marcas de nacimiento, etc.).

Según el número e importancia de los identificadores intrínsecos que las Autoridades Certificadoras verifican, registran y archivan para la emisión de sus certificados de identidad, diferente será la confianza que éstos puedan ofrecer. Una Autoridad de Certificación puede requerir sólo el DUI y comprobar que la fotografía y la apariencia del solicitante coinciden, otra puede exigir, además o en lugar de, un requerimiento notarial, otra las huellas dactilares, etc.

Cada Autoridad de Certificación, publica cuales son los requisitos y el protocolo a seguir para obtener cada uno de los tipos de certificados digitales que componen su oferta, de forma que, quién verifica el certificado de la clave, pueda establecer cual es el nivel de confianza que le merece dicha clave pública y el correspondiente usuario.

### 4.3.3 EMISIÓN DE CERTIFICADO

Una Autoridad de Certificación puede ser cualquier organización o institución que se comprometa a ser garante de los extremos que aparecen en sus certificados y en su política de seguridad.

Así, cualquier empresa puede actuar como una Autoridad de Certificados de Identidad a favor de sus empleados, o una universidad de sus estudiantes, etc, ya que, previamente, estos organismos e instituciones han aplicado diferentes

protocolos de identificación a sus miembros, con lo que la emisión de certificados digitales sólo es una extensión de los certificados clásicos que ya expedía.

Además de los compromisos de verificación que se indican en la política pública de una Autoridad de Certificación, ésta se compromete a emitir documentos digitales (los certificados) únicos y perfectamente identificables a través de su número de serie. Dichas autoridades también son responsables de mantener un registro seguro y disponible, sobre cual es el estado de cada uno de los certificados que emite. Un certificado digital siempre está en alguno de los siguientes estados:

- ✓ **Activo o Preactivo**: Por estado preactivo se entienden aquellos certificados que, generados en un determinado instante, sólo serán válidos en un intervalo de tiempo posterior. Desde el momento en que se genera el certificado y hasta que llega el momento de entrar en vigencia, el certificado está en estado Preactivo. Cuando la fecha en curso está dentro del intervalo de vigencia de un certificado, en este caso, decimos que está en estado Activo.

- ✓ **Suspendido**: Muchas veces es necesario anular temporalmente la vigencia de un certificado, para ello, la Autoridad de Certificación emisora decide pasarlo al estado de Suspendido. Con ello no se está invalidando de forma irreversible el certificado, sino que se le retira de circulación hasta que se le vuelva a dar el estado de Activo.

- ✓ **Revocado**: Cuando las condiciones que llevaron a la emisión de un certificado cambian antes de que éste expire, y son de importancia suficiente, la Autoridad de Certificación deberá anularlo; para ello, emite un segundo certificado especial, denominado “de revocación”, por el cual, desde ese instante desautoriza al certificado previo y lo hace de un modo irreversible.

Funcionamiento.

**a)** Imaginemos un estudiante universitario al que se le autoriza utilizar determinados recursos durante el periodo de prácticas de una determinada asignatura. El certificado de autorización lo puede emitir Jefatura de Estudios al principio del curso y, sin embargo, el periodo de prácticas para ese alumno puede caer a la mitad del curso académico.

**b)** Pensemos en el caso de un empleado que dispone de diferentes certificados de autoridad y que va a disfrutar de su periodo de vacaciones, para su mayor seguridad, antes de irse, solicita a la Autoridad de Certificación que suspenda todos sus certificados de autoridad ya que él no va estar en la empresa y no hay modo lícito por el cual puedan utilizarse dichos certificados para ejercer la autoridad que declaran.

**c)** En el caso de ser revocado, veamos el de un funcionario público que ha sido retirado de su cargo e inhabilitado para desempeñar sus funciones, al que la Autoridad de Certificación correspondiente le invalida todas sus credenciales relacionadas con su condición previa.

- ✓ **Caducado**: Este es el estado final de cualquier certificado y se produce cuando la fecha en curso es posterior a la fecha de caducidad indicada en el propio certificado. El estado de “certificado caducado” no le resta valor histórico ya que, mientras estuvo activo, las operaciones en las que participó eran perfectamente válidas. Las Autoridad Certificadora deben tener en todo momento registrado cuales son los estados en los que se encuentran sus certificados. En la literatura general sobre Terceras Partes Confiables o TPC, se habla de las “Listas de Certificados Revocados” como unas listas “negras” en las que la entidad emisora pública a los cuatro vientos cuales son los certificados que ha anulado para, con ello, desentenderse de las

responsabilidades que pudieran acarrear la utilización y/o aceptación por parte de algún agente de la red de los mencionados certificados. Según la importancia de las transacciones que realicen los agentes basándose en los certificados digitales que utilizan, algunas veces no será necesario que consulten si las credenciales presentadas están todavía vigentes en el momento de la transacción, pero habrá otros casos en los que este requisito sea absolutamente necesario, por lo que el agente verificador se pondrá en contacto con la Autoridad de Certificación emisora de la credencial y le preguntará por el estado de vigencia (actividad) de ese certificado en concreto (número de referencia). Por su parte, la autoridad consultada deberá devolver al consultante un documento firmado y fechado con la información solicitada.

### 4.3.4 ALMACENAMIENTO EN LA AC DE SU CLAVE PRIVADA

Las Autoridades Certificadoras vistas como un todo, se encargan de verificar las condiciones que aparecen en sus políticas públicas de seguridad y, posteriormente, de emitir y seguir el ciclo de vida de los certificados que emite.[84]

En cuanto a esta última actividad, las Agencias de Certificación son firmantes digitales, para lo cual deben disponer de una clave privada que sólo conocen ellos y que custodian con niveles de seguridad iguales o superiores a los declarados públicamente.

Dado que todo el valor reside en que cada Agencia de Certificación es la única capaz de generar las firmas que llevan su identificador, es muy importante que esas claves privadas se almacenen y gestionen de forma segura. Cualquier falla

[84] (En algunos textos, ambas funciones se consideran por separado y lo que aquí denominamos Autoridad de Certificación en sentido amplio, allí lo dividen en Autoridad de Certificación y Autoridades de Registro. Las funciones de evaluación y verificación de los extremos contenidos en la política de seguridad se le atribuyen a las Autoridades de Registro que pueden ser varias, y la capacidad de emitir certificados digitales se delega a la Autoridad de Certificación propiamente dicha. En este caso, las Autoridades Certificadoras actúan como agentes ciegos guiados por las Agencias de Registro).

en la seguridad de las claves privadas no sólo pone en entredicho a la institución, sino que invalida todos los certificados emitidos por ella.

Para conseguir este nivel de seguridad para las claves privadas, éstas se generan y almacenan permanentemente en unidades hardware de alta seguridad, sometidas a sofisticadas medidas de seguridad física y dentro de entornos a prueba de intrusión electrónica. A dichas unidades se las denomina “Unidades de Firmado de Certificados” o CSU.

Estas unidades son, por su naturaleza, irrepetibles, y están diseñadas para que, ante la sospecha de cualquier intento de intromisión, las claves y demás informaciones relacionadas con ellas se destruyan antes de que puedan ser alcanzadas desde el exterior.

Las CSU están físicamente resguardadas para evitar ataques electromagnéticos, y tienen un amplio conjunto de censores tolerantes a fallos permanentemente a la escucha de cualquier síntoma que pueda indicar la existencia de un ataque. Los administradores de la Autoridad de Certificación no tienen acceso a la clave privada, sino a un equipo hardware que firma los documentos que éstos le entreguen.

En algunas implementaciones actuales, la CSU se activa mediante un conjunto de “llaves de datos”, las cuales son objetos físicos capaces de almacenar información digital. Estas llaves utilizan lo que en la terminología criptológica se denomina “compartición de secretos”, y que conduce a protocolos en los que varias personas deben utilizar al tiempo sus llaves de datos para activar la CSU.

Esta política clásica de reparto de la autoridad impide que un solo administrador pueda concentrar un nivel de autoridad tal que, le permitiese producir certificados

fuera del protocolo público declarado para esa Autoridad de Certificación; estos certificados serían “falsos” aunque haya sido la misma instalación los que los haya producido.

En caso de incendio o cualquier otra catástrofe involuntaria y fortuita, si la CSU se destruye la validez y autenticidad de los certificados y credenciales emitidos no queda comprometida y los certificados firmados por la CSU siguen siendo válidos.

Esto es así siempre y cuando la estructura de la CSU asegure que las claves privadas fueron completamente destruidas en el incidente y que de sus restos no se puede obtener información parcial o marginal alguna de cuales fueron esas claves.

Algunas CSU se van a instalar pensando en que si la clave privada se pierde, ésta se pueda volver a recuperar e instalar en una nueva unidad. Por ejemplo, RSA Data Security Inc. tiene en el mercado una unidad hardware para la emisión de certificados creada por BBN (Bolt, Beranh y Newman) y que sigue esta filosofía.

La posibilidad de que las claves privadas puedan ser reconstruidas en otras unidades tiene como objetivo poder mantener una identidad digital más allá del período de vida del equipo que la ejerce.

Mientras que esta cualidad puede entenderse como una ventaja, también hay que tener presente que abre una puerta a la posible “clonación” de identidades digitales, lo cual está frontalmente en contra de la misma razón de ser de las Autoridad Certificadora.

### 4.3.5 MANTENIMIENTO DE LAS CLAVES VIGENTES Y REVOCADAS

Las Autoridades Certificadoras pueden, dentro de los servicios que ofrecen al público, almacenar los certificados emitidos durante su período de validez.

De este modo, en el caso de que uno de los suscriptores pierda su certificado, siempre podrá pedirle a la autoridad emisora, que le envíe de nuevo una copia.

También se ofrece este servicio en aquellas Autoridades Certificadoras que tienen asociados, servidores públicos de certificados, mediante los cuales cualquier suscriptor puede solicitar los certificados de cualquiera de los demás suscriptores.

Este tipo de servicios son especialmente importantes en las Autoridades Certificadoras dedicadas a la emisión de Certificados de Identidad Personal, ya que cualquier suscriptor que quiera establecer contacto con otro desconocido, tan sólo tendrá que obtener su certificado de identidad y enviarle un mensaje de correo electrónico utilizando la clave que aparece en el certificado.

De este modo, el agente se asegura de que, de leer alguien el contenido de su mensaje, éste sólo podrá ser el poseedor de la identidad que él espera.

La disponibilidad pública de los certificados electrónicos, para algunos supone, además de una ventaja, un riesgo.
Al mantener expuestas las claves, cualquiera podrá tomarlas y someterlas a un ataque; por ejemplo, de factorización, en el caso de las claves RSA, o del cálculo de logaritmos discretos en el caso del DSS.

Para evitar con cierto éxito (prácticamente total), que estos ataques puedan obtener resultados provechosos para el atacante, todo par de claves pública y privada, tienen un tiempo de vida limitado.

Este período se establece según sea la complejidad computacional del ataque, como se prevé que evolucione la tecnología durante ese tiempo y cual sea el nivel de uso previsto para esa clave.

Aunque pueda parecer extraño por ser de naturaleza inmaterial, las claves criptográficas se desgastan con el uso al igual que lo hacen los materiales físicos que nos rodean.

En cualquier verificación de una firma, siempre se debe comprobar la fecha de caducidad y el momento en el que estamos; en ningún caso se deben aceptar mensajes firmados con fecha pasadas, y en los casos de riesgo es mejor exigir que los mensajes estén temporalmente certificados (estampillados o matasellados) por alguna o algunas Autoridad Certificadora independientes dedicadas a ese menester.

En el caso de que un usuario quiera rectificar una clave previamente caducada, deberá asegurarse de que ésta tiene suficiente longitud (en dígitos) y que no hay indicios de que haya sido comprometida.
En este caso, lo que hace la Autoridad de Certificación es comprobar que el solicitante es realmente el poseedor de la clave privada asociada con la clave pública que se le presenta, y emitir un nuevo certificado para la misma clave y las nuevas firmas se referirán al nuevo certificado, en lugar del anterior.

De todas formas, y aún siendo este proceder aceptable en escenarios de seguridad media, la facilidad con la que se generan claves hace innecesario mantener vigente una clave durante períodos de tiempo mayores que los especificados cuando se certificó por primera vez.

Cuando se destruye voluntaria o involuntariamente una clave privada que no haya sido comprometida, desde ese momento no se pueden firmar ni descifrar mensajes con ella, si bien todos los documentos firmados antes de la pérdida permanecen válidos.

Dado que la clave pública asociada, sigue estando dispersa por la red, el titular de la clave deberá solicitar a las Autoridades Certificadoras que hayan emitido certificados para ella, que los revoquen.

De este modo se pretende evitar que alguien pueda seguir utilizándola para enviar mensajes cifrados al titular y éste ya no podrá leerlos.

Dentro de la política de seguridad de cualquier Autoridad de Certificación que se precie, deben indicarse cuales son las medidas de seguridad y protocolos a seguir cuando se den este tipo de situaciones.

En el caso, aún peor, de que la clave haya sido develada, o se sospecha que un posible atacante puede obtenerla total o parcialmente, el titular de esa clave debe notificar inmediatamente tal extremo a las Autoridades Certificadoras que hayan emitido certificados a su favor y con esa clave.

La autoridad pasará a incluir inmediatamente dicha clave en sus Listas de Certificados Revocados, con la esperanza de que esa invalidación se difunda rápidamente a través de los usuarios habituales o fortuitos de esa clave.

A continuación, el titular legítimo debe generar un nuevo par de claves y obtener el certificado correspondiente.

La nueva clave puede utilizarse para “volver a firmar” los documentos que habían sido firmados con la clave anterior, ahora comprometida, como reafirmación de los compromisos anteriores. Hay que tener muy en cuenta que el efecto de la revocación de un certificado tiene efecto a partir del momento en el que aparece en la LCR (Listado de Certificados Revocados) de la Autoridad de Certificación emisora y que invalida cualquier operación que se haga con fecha posterior, sin embargo, no afecta a las operaciones anteriores.

Esto es así para evitar que un suscriptor, declarando su clave comprometida, se pueda desdecir de lo que firmó con anterioridad a la fecha de la denuncia.

Como puede darse el caso de que el titular sea realmente honrado y que el atacante que ha comprometido la clave pueda emitir firmas con cualquier fecha, los sistemas serios en los que es fundamental la cualidad de no repudio, las fechas de firma y los propios documentos firmados, deben ser certificados temporalmente, matasellados, por agencias completamente imparciales dedicadas a tal fin.

### 4.3.6 SERVICIOS DE DIRECTORIO

En el caso de que alguien quiera encontrar la clave pública de un usuario del sistema, existen diversas formas de conseguirlo: bien por teléfono, por correo común o de superficie, consultando publicaciones periódicas, etc., sin embargo, estos métodos, aún pudiendo ser muy seguros, adolecen de una lentitud a veces intolerable.

Para poder obtener esa misma información a la velocidad habitual de las redes, las Autoridades Certificadoras dan Servicios de Directorio mediante los cuales, cualquiera puede obtener la clave pública certificada de cualquier miembro con quien quiere ponerse en contacto o establecer relaciones de algún tipo.

Un Servicio de Directorio consiste en una gran base de datos en la que cada entrada de usuario en el directorio (DIT o Directory Information Tree) contiene los certificados de las claves públicas de las que es titular, y cada entrada de una Autoridad de Certificación contiene todos los certificados;

**1)** Emitidos para ella por otras Autoridad Certificadora ante las que está inscrita, y

**2)** Todos los certificados emitidos por ella misma para otras autoridades.

Los Directorios hacen las funciones de las “guías telefónicas” y deben de estar protegidos contra accesos no autorizados, de forma que los usuarios puedan obtener de ellos los certificados de las claves públicas que necesiten.

De no existir este tipo de servicios, la distribución de los certificados y credenciales debería hacerse a través de canales de comunicación ajenos a la red con lo que haría más lenta la velocidad de operación de todos los suscriptores y quedarían muy reducidas las ventajas iniciales de los métodos telemáticos.

### 4.4 IMPORTANCIA DE LA AUTORIDAD DE CERTIFICACIÓN.

Es necesario establecer una estructura que brinde confianza a las transacciones, no solo desde el punto de vista técnico sino también jurídico.

Las autoridades juegan un papel definitivo tanto para brindar seguridad en la red, como para asegurar la confianza en el mundo físico, respecto a algunos de los actos que tengan efectos jurídicos que en ella se den. “Esto significa que se podrá realizar convenios y transacciones comerciales sin necesidad de viajar fuera del país e incluso sin moverse de su puesto de trabajo, pues todas las operaciones las podrá realizar desde su computadora. Obtendrá la seguridad de que conoce la identidad de aquel con quien está negociando, tendrá certeza de que el

documento enviado no ha sido manipulado, ni alterado y una vez la otra persona recibe el mensaje, este hecho no podrá ser negado."[85]

Esta Autoridad Certificadora también permiten conocer a los emisores de una oferta y aceptación de actos jurídicos y las partes intervinientes en un contrato. Además evitaN que se cometan fraudes por falsificación de identidad o que se caigan en errores contractuales por falta de personería jurídica.

La Autoridad Certificadora, por el vinculo que tienen en la transmisión de los mensajes de datos, brindan precisión sobre el autor y contenido sobre un mensaje de datos, así mismo de ellas depende el desarrollo de canales de comunicación seguro en esta era de aumento del comercio electrónico. *"Constituye además una especie de fedatario ya que se convierte en un tercero disipador de conflictos al determinar la originalidad y autoría de los mensajes de datos."*[86]

**4.5 SISTEMA DE CERTIFICACIÓN.**

El sistema de certificado ha de basarse en una serie de puntos esenciales, que son los siguientes:

La vinculación de forma segura de una clave pública a una persona determinada, es el papel central de toda entidad de certificación, que debe responder por esta actuación, y la función esencial de todo certificado.

La importancia de la correcta identificación del solicitante, es que en algunos casos ésta es defectuosa y puede llegar a darse la existencia de firmas falsas por suplantación de la persona del solicitante del certificado por parte de un tercero.

[85] Guerrero, María Fernanda. El notario virtual de los negocios en línea. Revista Ámbito Jurídico. Bogota, Colombia, Abril 2001. Pág 12
[86] Op. Cit. Cubillos Velandia, Pág 257

El control de la correspondiente clave privada por parte del titular del certificado al que se ha vinculado con una determinada clave pública es también esencial para evitar supuestos de falsificación de firma por utilización no autorizada por parte de terceros en caso de pérdida y robo de la clave de firma.

De aquí deriva la importancia de una existencia de sistemas de revocación que permitan comunicar que una determinada clave deja de estar vinculada, y por tanto, no le son ya atribuibles los mensajes firmados con la misma.

La existencia de sellos temporales digitales de confianza es esencial para el correcto funcionamiento, fundamentalmente, para determinar el momento de creación de mensajes electrónicos durante el período de validez del certificado.

El sistema de certificados debe estructurarse, dada la naturaleza transfronteriza del comercio electrónico, de forma tal que sean a través de una adecuada jerarquización de las Autoridad Certificadora.

Es decir que existe un reconocimiento general de los certificados. Solo de ésta forma y teniendo en cuenta éstas bases se podrá conseguir un sistema útil, eficaz y seguro, y por lo tanto la tecnología que utiliza la Firma Electrónica con la adecuada infraestructura legal e institucional, puede ser una alternativa poderosa de base informática a las firmas tradicionales.

**4.6 NATURALEZA JURÍDICA.**

La naturaleza de las Autoridad Certificadora está abierta de acuerdo a la legislación en la que radique, así podrán ser públicas o privadas, y su funcionamiento estar sometido a una autorización o ser de libre constitución.

Se señala como una ventaja el hecho de que la entidad de certificación sea pública, ya que su objetivo es el beneficio de la comunidad y por ende un mejor servicio.

Se presume que una administración o una entidad pública actuará en función del interés público, además de ser más estable que las privadas.

“Las Autoridad Certificadora públicas pueden desempeñar distintos papeles: pueden actuar como autoridad de certificación raíz de la estructura de autoridad de certificación de un país, certificando al resto de Autoridad Certificadora comerciales, o bien pueden actuar como Autoridad Certificadora para los ciudadanos únicamente, para las relaciones administrador-administrados.”[87]

Resulta lógico que para que una entidad de certificación pública funcione adecuadamente, es necesario que el Estado tenga la voluntad de incorporar esa tecnología al organismo público que asuma esas funciones de certificadora, o de legarlas a algún organismo que cuente con la infraestructura y sea capaz de asumir esa responsabilidad.

La Autoridades Certificadoras pueden ser autoridades privadas, dependiendo de la legislación en cada país. Una empresa privada fundamentalmente buscaría el lucro y se trata de un régimen de competencia en el que de acuerdo a la calidad de sus servicios pueden ampliar el número de usuarios de sus certificados, dependiendo de la seguridad que les ofrezca.

“Dentro de las funciones de las autoridades privadas, tenemos que pueden dedicarse a la certificación, ofreciendo ese servicio a terceros como parte de su

[87] Op. Cit. Martínez Nadal, “Comercio Electrónico...” Pág 151

actividad empresarial principal, o bien únicamente de forma complementaria a esa actividad o a efectos internos puramente organizativos"[88]

Para que una empresa privada se constituya como entidad de certificación, es necesario que cumpla con los requisitos que la ley ha previsto para garantizar la seguridad a los usuarios del comercio electrónico. Estos requisitos están consignados en las normas que regulan la prestación de estos servicios en cada país.

## 4.7 REQUERIMIENTOS DE LAS AUTORIDADES CERTIFICADORAS.

Para que una entidad certificadora pueda considerarse confiable, debe cumplir una serie de requisitos fundacionales, así como otros requisitos posteriores de funcionamiento que genera una confianza y seguridad en su organización y actividades. En la medida que la empresa certificadora cumpla con todos los requisitos exigidos, tendrá mayor solidez ante la vista del usuario de que otra certificadora solo cumpla con algunos de ellos.

Doctrinariamente, se logra un consenso sobre los requisitos que deben cumplir las Autoridad Certificadoras; clasificándolas básicamente de la forma siguiente:

**1.** Requisitos técnicos:

Estos consisten en la utilización de sistemas seguros y de confianza por parte de la Autoridad de Certificación para el desarrollo de sus actividades. Por ejemplo, para emitir, suspender o revocar un certificado, publicar o dar noticia de la emisión, suspensión o revocación de un certificado, o para crear o salvaguardar su propia clave privada.

[88] Op. Cit. Martínez Nadal, "Comercio Electrónico..." Pág 151

**2.** Requisitos de personal:

El personal que labora en la autoridad certificadora debe ser competente desde el punto de vista de gestión, técnica y confianza. El personal que tiene acceso a las operaciones criptográficas, emisión, suspensión o revocación de los certificados digitales, deberá someterse a una investigación inicial para determinar si puede acceder a una posición de confianza, con la finalidad de proporcionar seguridad y confiabilidad a sus usuarios.

**3.** Requisitos financieros:

Es necesario que la entidad certificadora cuente con un capital base que servirá para desarrollar el negocio y para afrontar eventuales responsabilidades por daños, por error o negligencia, o como consecuencia de cualquier acción u omisión de la Entidad Certificadora.

**4.** Auditoria:

Para mostrar la fiabilidad de la autoridad de certificación, deberá someterse a una Auditoria.

**5.** Documentación de actividades:

La documentación de actividades es indispensable para la actuación de una autoridad de certificación digna de confianza. Esta debe ser capaz de probar sus propias operaciones y actuaciones en el futuro. La documentación debe ser conservada durante un periodo adecuado, el cual debe estar fijado en el contrato de prestación de servicios, la practica o incluso en la ley, y el cual puede ser variado de acuerdo a la necesidad del usuario.

**6.** Planes de contingencia y de recuperación frente a desastres:
La entidad certificadora debe estar preparada ante la posibilidad de una paralización del funcionamiento de sus sistemas, lo cual, de no poseer dichos planes acarrearía graves consecuencias para los usuarios de los certificados.

**7.** Finalización de actividades con los mínimos perjuicios a sus usuarios:
Cuando una entidad certificadora finaliza sus actividades, es decir, que cesará en la prestación de sus servicios, deberá avisar anticipadamente a sus clientes a fin de evitarles perjuicios, a la vez que puede ofrecerles traspasar sus actividades a otra entidad certificadora previamente calificada.

## 4.8 OBLIGACIONES DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN.

Como hemos citado anteriormente las bases y requisitos de las Autoridades Certificadoras, es el momento de hablar de las obligaciones que tiene en su rol, de prestador de servicios de certificación.

Entre estas exigencias enfatizaremos el hecho de controlar en todo caso y en todo momento la fiabilidad del certificado, identificando a quien se le va a otorgar, y una vez otorgado, manteniendo un registro de los certificados emitidos y poniendo a disposición de los signatarios, los dispositivos de creación y verificación, y no almacenar ni copiar los datos de creación de firma de la persona a la que hayan atendido.

Otras obligaciones están inclinadas a garantizar los certificados, en cuanto al contenido, tiempo, día y hora de emisión, además, emplear personal calificado y utilizar sistemas y productos viables para que se garantice las medidas de seguridad contra la falsificación de certificados.

Estas obligaciones se complementan con el deber que tiene el prestador de servicios de certificación, de disponer de recursos económicos para afrontar el riesgo de la responsabilidad por daños y perjuicios.

**4.9 RESPONSABILIDAD DE LAS AUTORIDAD DE CERTIFICACIÓN:**

La responsabilidad de las Autoridades Certificadoras al desarrollar una verdadera vocación de servicio al público, debe adoptar la figura del buen padre de familia, respecto a la ejecución misma de su labor, de modo que todo incumplimiento por parte de la entidad se convierta en culpa o falla en la prestación del servicio, y por ende sea una causal de responsabilidad. Es decir, que el prestador de servicios de certificación responde por los daños y perjuicios causados en el ejercicio de su actividad, con independencia de si su actuación fue diligente o negligente, o sea, que si el prestador de servicios tendrá que responder no solo en el caso de que se haya debido a la negligencia de sus empleados –por ejemplo, no exigieron el documento acreditativo de la identidad del titular- sino que el error se haya producido pese a haber actuado con diligencia; pero esto no quiere decir que el proveedor de servicios no será responsable si puede demostrar que no ha sido negligente, por ejemplo, probando que ha tomado medidas razonables para evitar errores en el certificado reconocido.

"Es por ello que se puede aplicar la responsabilidad objetiva, es decir, un régimen en el cual no se analiza al sujeto responsable (caso de responsabilidad subjetiva), si no exclusivamente a los hechos, sin entrar a examinar la condición subjetiva del agente".[89]

Tomando los dos supuestos de responsabilidad – objetiva y subjetiva – y teniendo en cuenta las dificultades que para el usuario de un certificado puede suponer la

[89] Op. Cit. Cubillos Velandia, Pág 296

prueba de la negligencia de la entidad certificadora, se establece la carga de la prueba para las Autoridad Certificadora.

Una segunda responsabilidad está dada por su naturaleza contractual o extracontractual. La entidad certificadora tiene como obligación establecida el contrato mismo, y como accesoria a éste, la de dar información y por lo tanto, en caso de incumplir con cualquiera de éstos, produciría una responsabilidad para la entidad certificadora; por desarrollar éstas el principio de buena fe, el cual incluye no sólo el tener la convicción por parte del contratante de actuar adecuadamente, si no que además implica el desarrollar aquellas actividades que el co-contratante requiera para que se dé cabal cumplimiento al objeto del contrato.

Por la evolución de la responsabilidad contractual, se ha generado un debilitamiento en la autonomía de la voluntad ya que las empresas incluyen en sus contratos cláusulas exonerativas de responsabilidad. De tal manera que en caso de controversia de un contrato que incluya este tipo de cláusulas, el juez está en la obligación de analizar el fondo del contrato y determinar cuales son las obligaciones del mismo, y en caso de ser necesario deberá obviar la existencia de dichas cláusulas, si en virtud de ellas, la entidad certificadora está contraviniendo una obligación que pertenece a la naturaleza misma del contrato.

Como consecuencia de lo anterior, el juez le otorga al contrato una serie de obligaciones que aunque no se encuentren presentes dentro del mismo, deberían haber estado, son obligaciones implícitas a la ejecución del contrato mismo.

En conclusión, respecto a la responsabilidad contractual, se debe en principio acudir al contenido estricto del instrumento, entendiéndose que dicho contenido incluya las obligaciones esenciales y las obligaciones accesorias necesarias para el cumplimiento del mismo, de modo que si éste no las contiene, deberán hacerse

valer, en razón de la justicia, por tratarse de obligaciones implícitas a la ejecución del contrato.

## 4.10 AUTORIDADES PÚBLICAS DE CERTIFICACIÓN A NIVEL INTERNACIONAL

La estructura y el cuadro de funcionamiento de las Autoridades Certificadoras "public key infrastructure" prevén generalmente una estructura jerarquizada a dos niveles: El nivel superior suele estar ocupado por las autoridades públicas, que es la que certifica a la autoridad subordinada, normalmente privada.

### 4.10.1 EN ESPAÑA

Está 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 a todos los efectos legales del certificado digital, algo que aún no se contempla en nuestra legislación.

Los servicios que está previsto 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.

Los Notarios y Corredores de comercio, a través de sus colegios respectivos, en un intento de acomodar estatus a los nuevos tiempos virtuales, han tomado parte activa en lo relativo a su condición de fedatarios públicos.

Este proyecto no ha tenido el éxito que se esperaba, en el ámbito privado quien lleva la delantera es la Agencia Certificadora ACE (de carácter privado, que agrupa a varias empresas del sector)

### 4.10.2 EN ITALIA

Parece ser que la autoridad nacional de certificación será la AIPA (Autoritá per l'Informática nella Pubblica Amministrazione).

## 4.11 AUTORIDADES PRIVADAS DE CERTIFICACIÓN

### 4.11.1 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 y recientemente BBVA.

### 4.11.2 EN BÉLGICA

Existe el Tercero Certificador llamado Systéeme Isabel, que ofrece servicios certificadores a socios financieros y comerciales.

La Cámara de Comercio unida a la empresa VERISIGN ha formado un Trusted Third Party en el cual la Cámara de Comercio hace las funciones de Registro y VERISIGN hace las funciones de emisión de certificados y técnicas.

### 4.11.3 EN ESTADOS UNIDOS

- NETSCAPE: Los servicios de seguridad de redes (NSS) en alianza con la empresa SUN, producto "l-planet" (PKI)

- VERISIGN: Servicios de autenticación con tecnología PKI. Ofrece el servicio de apoyo a empresas e instituciones que presten sevicios de certificación, bajo laadministración y software de Verisign. Asimismo ofrece la posibilidad de autenticar en Internet un sitio web o una Intranet, bajo identificación de los servidores SSL (estándar actual de credenciales).

- RSA: Proveedor de tecnologías de seguridad en cuanto a Autentificación (Secur

  ID); Autorización (Clear Trust) para la administración de privilegios de acceso;

Infraestructura de clave pública PKI (RSA Keon) para la administración de certificados y Encriptamiento (B Safe) para la protección de la información.

- BALTIMORE : Proveedor de tecnología de seguridad con el producto UNICERT formado por tres niveles de tecnología: Central (Autoridad Certificadora, Registro de Usuarios, PKI, Emisión y Administración de Certificados); Avanzada (Dotar de tecnología a autoridades certificadoras comerciales) y Extendida (Servicios de valor agregado adicionales como sellos cronológicos (time stamping)

### 4.11.4 EN INTERNET

Existen ciertos servidores en Internet conocidos como "servidores de claves" que recopilan las claves de miles de usuarios. Todos los servidores de claves existentes en el mundo comparten esta información, por lo que basta publicar la clave en uno de ellos para que en pocas horas esté disponible en todos ellos.

### 4.11.5 EN MÉXICO

1. Segurídata y Acertia (entidades privadas)
2. Banxico (entidad pública)

### 4.11.6 EN LA COMUNIDAD EUROPEA

La directiva encomienda la función de tercera parte de confianza encargada de dar seguridad a las firmas electrónicas, estableciendo un vínculo entre el elemento de verificación y una persona determinada a unas entidades que denomina proveedores de servicios de certificación (opción terminológica comunitaria, que pone de manifiesto una voluntad de evitar siquiera la apariencia de atribución de naturaleza pública que sí podrían sugerir otras denominaciones como, por

ejemplo, autoridad de certificación). El art. 2.6[90] define al proveedor de servicios de certificación como la persona o entidad que emite certificados o proporciona al público otros servicios relativos a la firmas electrónicas; tales servicios pueden ser inherentes al propio certificado y necesarios (revocación y suspensión en caso de pérdida de la clave privada u otro elemento de firma), otros más bien discutibles (generación de las claves, que el anexo II permite al proveedor, el cual puede también almacenarlas, con la autorización del usuario), así como otros complementarios pero igualmente necesarios para la seguridad del sistema de certificados en particular o del comercio electrónico en general.

### 4.11.7 EN EL SALVADOR

Desde Enero de 2002, existen mas de doscientos cincuenta usuarios realizando transacciones reales por Internet con la Dirección General de la Renta de Aduanas de El Salvador (Envío de la declaración de mercancía y póliza por Internet ), agilizando en gran medida el procesamiento de información para la importación de mercadería. Los principales usuarios son empresas de courier, agencias aduanales, maquilas y empresas industriales.

Para la implementación de este proyecto, el rol de DIESCO EAN-El Salvador, fue decisivo tanto para el desarrollo de la plataforma tecnológica y operativa de TELEDESPACHO como por los servicios cerrados de emisión de certificados digitales a través de su Autoridad Certificadora CERTICAMARA.[91]

Reformas a la Ley de Simplificación Aduanera, con el que se autoriza el funcionamiento de Autoridad Certificadora y la prestación de servicios de certificación para el sistema de Teledespacho; es decir para el sistema de

[90] Union Europea. Directiva del Parlamento Europeo y del Consejo porla que se establece un marco comunitario para la Firma Electrónica (1999)
[91] Esta entidad certificadora nace jurídicamente con el Decreto Legislativo Numero 523 del 30 de Agosto de 2001 publicado en el Diario Oficial Numero 353, del 5 de Octubre de 2001

certificación cerrada, en el cual el certificado es válido únicamente para transacciones con la Dirección General de Rentas y Aduanas.

Para el sistema de Teledespacho por Internet, se ha implementado el uso de la firma electrónica y certificados digitales, con el objetivo de asegurar las transacciones electrónicas de dicho proyecto. Estos mecanismos aseguran el envío y la recepción de la información, ya que el emisor al firmar el documento electrónico y validarlo con su certificado digital, está dotando a dicho documento de la característica de seguridad. Esto le da certeza al receptor de que quien firma y envía es quien dice ser, adicionalmente este mensaje se codifica para que viaje por Internet en un lenguaje en que solo las partes involucradas podrán entenderlo.

Cabe aclarar que por el momento, los certificados digitales emitidos por Certicamara solo certifican al usuario, no la información y su uso es únicamente para Teledespacho por Internet, es decir, tramites de importación por Internet con la Dirección General de la Renta de Aduanas.

Las practicas realizadas por Certicamara, han sido elaboradas en el contexto de la declaración de prácticas de certificación a que se refiere el proyecto de régimen uniforme para las firmas digitales, en relación con la Ley modelo sobre comercio electrónico, elaboradas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional y su finalidad es constituirse en el mecanismo formal de difusión y comunicación, para con los titulares de un certificado digital emitido por Certicamara, así como para con cualquier persona que pretenda usar y confiar en dichos certificados.

CERTICAMARA, es una autoridad certificadora de carácter privado y los certificados que emite son utilizados para el sistema de Teledespacho por Internet, facultad otorgada por el Ministerio de Hacienda, quien a su vez actúa como

autorizador, fiscalizador y sancionador de la entidad certificadora, conforme lo preescrito en el Art. 8 de la Ley de Simplificación Aduanera.

La finalidad de los servicios ofrecidos por Certicamara, es constituirse en un tercero de confianza para las partes involucradas en una transacción electrónica con la aduana, creando de esta manera un marco de seguridad jurídica y tecnológica para sus usuarios.

- **SERVICIOS**

Dentro de los servicios de certificación digital prestados por Certicamara, se encuentran:

- Emisión de certificados: ya sea que se trate de personas naturales o jurídicas.

- Revocación de certificados: se da por terminada la vigencia de un certificado anticipadamente, cuando el titular así lo desee, o cuando concurra alguna causal de revocación.

- Publicación de certificados: los certificados digitales emitidos deben ser publicados en un directorio, de manera que terceros interesados puedan acceder a ellos.

- Almacenamiento de certificados: por seguridad, los certificados emitidos y la lista de revocados, son almacenados por un período determinado de tiempo debido a que el documento firmado digitalmente, puede poseer un período de validez o vigencia mas amplio que el del certificado utilizado para firmar.

- **TECNOLOGÍA UTILIZADA**

La tecnología aplicada en los productos utilizados por Certicamara han sido creados utilizando el mas alto nivel de criptografía, siguiendo el modelo de

criptografía de clave pública mas reconocido y utilizado a nivel internacional, RSA. Con la implementación de esta tecnología, Certicamara ofrece a sus clientes el mas alto nivel de seguridad, consistentes en claves RSA de hasta 2048 bits[92] de extensión y claves simétrica de 128 bits de longitud. Las claves privadas se generan y almacenan en dispositivos de seguridad que cumplen con las especificaciones internacionales.

- **GENERACIÓN DE CLAVES**

La generación de las claves publica y privada necesarias en la emisión de un certificado digital, se realiza bajo el absoluto control de quien será el titular de dicho certificado y es de exclusiva responsabilidad de éste, el tomar las medidas de seguridad que considere necesarias para el resguardo de la clave privada y su respectiva contraseña de acceso.

---

[92] Definiciones de **Bits** en la web:

Acrónimo de Binary Digit (dígito binario).
es.wikipedia.org/wiki/Bits

Término proveniente del inglés Bit, acrónimo de Binary Digit: Código Binario, que designa la cantidad mínima de información, memoria necesaria, o trozo de información que puede fijar sin equívocos el conjunto de los elementos del mensaje a la elección entre dos alternativas igualmente probables (par o impar, sí o no).
www.monografias.com/trabajos16/diccionario-comunicacion/diccionario-comunicacion.shtml

- Un número binario codificado como dato. Un bit puede ser un “uno” o un “cero”
www.hidcorp.com/espanol/page.php

palabra que significa símbolos o dígitos binarios; proviene de binary digits; es también una medida de la cantidad de información contenida en un mensaje, definida por CE Shannon.
omega.ilce.edu.mx:3000/sites/ciencia/volumen3/ciencia3/149/htm/sec_11.htm

Un BIT (contracción de Binary digIT) es la parte más pequeña de información que es capaz de procesar un ordenador. Representa la existencia o ausencia de la electricidad o magnetismo en un punto determinado. Se representa mediante un 0 o un 1.
dewey.uab.es/pmarques/glosario.htm

- **USO Y VERIFICACIÓN DE CERTIFICADOS**

Gracias a la tecnología que sustenta la prestación de los servicios de certificación digital que ofrece Certicamara, el cliente puede tener la confianza que su certificado digital lleva impreso confidencialidad, autenticidad, integridad y no repudiación de la información que envíe o reciba a través de medios electrónicos. La responsabilidad sobre la adecuada utilización, alcance y repercusión en el uso de un certificado digital, recae exclusivamente sobre el titular del mismo.

- **USO Y PUBLICACIÓN DE LA BASE DE DATOS**

La información proporcionada por los usuarios de los servicios de certificación y la proporcionada por los titulares de los certificados digitales, no será revelada, compartida, rentada o vendida a terceras personas o empresas, bajo ninguna circunstancia.

Certicamara se reserva el derecho de revelar información, sin autorización del titular, cuando sea necesario para identificarlo, contactarlo o ejercer cualquier acción legal en su contra, o en caso de que alguna autoridad jurisdiccional o administrativa facultada para exigir dicha revelación, se lo solicite expresamente.

- **CONTROLES DE SEGURIDAD**

Para la prestación de los servicios de certificación digital, y en la emisión, administración, almacenamiento y revocación de certificados digitales, Certicamara cuenta con tecnología, mecanismos y procedimientos de seguridad del mas alto nivel, los cuales son revisados y actualizados con cierta regularidad. La seguridad es revisada y evaluada en términos de instalaciones físicas, de telecomunicaciones, de hardware, de software y de personal.

- **GARANTÍAS**

Certicamara otorga garantías respecto a los certificados digitales emitidos, pero aplican única y exclusivamente a los usuarios y titulares de los mismos, más no incluye a cualquier otro tercero participante. Responderá en razón del tipo de certificado de que se trate, lo cual analizaremos al referirnos a los certificados digitales.

- **RESPONSABILIDADES**

Certicamara no ofrece garantía expresa ni tácita sobre sus servicios de certificación digital y no será responsable por los daños o perjuicios que sufran sus usuarios, cuando éstos se deriven de la mala utilización de los servicios o por la presentación de documentación falsa por parte del usuario.

En los casos en que Certicamara tendrá responsabilidad, ésta estará delimitada por las consecuencias legales y económicas que deriven del cumplimiento o incumplimiento de los requisitos establecidos para los distintos procesos y niveles de certificación.

- **EXCLUYENTES**

Certicamara reconoce como excluyentes de responsabilidad las siguientes causas:

**a.** Cuando el daño o perjuicio se derive de la mala o indebida utilización de los servicios de certificación digital por parte de los usuarios finales; de la mala o incorrecta interpretación, análisis, síntesis o conclusión a que los usuarios finales lleguen en el uso de dichos servicios, e incluso si el solicitante de un certificado digital aporta datos o documentos falsos para la obtención de dicho certificado.

**b.** Cuando la interrupción o alteración temporal de los servicios de certificación sean por causas ajenas a su voluntad, fuerza mayor o caso fortuito, propiciada por

condiciones climatológicas adversas, fallas en la energía eléctrica, fuego, actos vandálicos, huelga o cualquier otro motivo similar que afecte sus instalaciones, así como por errores, omisiones o negligencia que afecten las instalaciones de transmisión, enlace y bases de repetición de los proveedores de telecomunicaciones de Certicamara.

**c.** Cuando la interrupción temporal del servicio sea ocasionada por acciones gubernamentales que coarten o restrinjan la libertad en las telecomunicaciones civiles o que impidan su transmisión privada o incluso, por cualquier otro motivo de naturaleza análoga.

- **SOLUCIÓN DE CONFLICTOS**

Cualquier controversia que se suscite entre Certicamara y sus usuarios, se resolverá a través de la negociación entre sus representantes comerciales.

Si no logra resolverse por este medio, se someterá a un arbitraje de derecho en el Salvador. Las reglas del arbitraje serán las del Centro respectivo de la Cámara de Comercio e Industria de El Salvador, o si no existiere, las reglas que contiene el reglamento de la UNCITRAL.

Los costos y honorarios razonables relacionados con el procedimiento arbitral serán cubiertos por ambas partes conjuntamente y por montos iguales.

### 4.11.8 REGULACIÓN JURÍDICA DE LA ENTIDAD CERTIFICADORA SALVADOREÑA.

La utilización de sistemas informáticos para el intercambio de información de trascendencia tributaria y la implementación de redes abiertas para dicho intercambio, hace necesaria la adopción de mecanismos de seguridad. Y dentro de este proceso de modernización, el Estado salvadoreño ha dictado

disposiciones pertinentes a fin de dar cobertura legal a las nuevas figuras que se han generado en la implementación de Teledespacho y de la entidad certificadora Certicamara, es así que se crea la Ley de Simplificación Aduanera.

Esta normativa tiene por objeto establecer el marco jurídico básico para la adopción de mecanismos de simplificación, facilitación y control de operaciones aduaneras, a través del uso de sistemas automáticos de intercambio de información, de acuerdo al Art. 1 de esta ley.

El Art. 6 de la ley, introduce la declaración de mercancías mediante transmisión electrónica de la información, a lo cual se le denomina Teledespacho, el cual está definido en el inciso 2º del mismo artículo de la siguiente manera: *"conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten, dentro de un marco de mutuas responsabilidades y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la Dirección General y los usuarios y auxiliares del servicio aduanero, bancos y en general, los operadores e instituciones contraloras del comercio exterior".*

El art. 7 inciso 1º de la ley de Simplificación Aduanera, establece que el intercambio de información que se brinda sobre las mercancías y otros documentos, así como para certificar el pago de lo adeudado por medios informáticos y de la vía electrónica goza de plena validez y produce los mismos efectos jurídicos que los entregados en soporte físico. El inciso 2º del mismo artículo plantea el caso de disconformidad de datos en un mismo documento registrado y presentado en la aduana, lo cual se resuelve considerando como correcto los datos sobre los cuales la entidad certificadora otorga fe publica, o si no, aquel que conste en documento escrito sin ninguna alteración, tachadura o borrón.

El establecimiento de los sistemas de certificación de la información para garantizar la autenticidad, confidencialidad, integridad y no repudio de la misma, está autorizada en el Art. 8 de la Ley, a través de la intermediación de empresas que proveen estos servicios, a los que denomina: Autoridad Certificadora.

La Autoridad Certificadora opern bajo la autorización del Ministerio de Hacienda, quien además ejerce funciones de fiscalizador y sancionador, mientras no se dicte una ley específica al respecto.

Las Autoridades Certificadoras que se autoricen para operar, se encargarán de emitir los respectivos certificados que permitan a los usuarios del sistema una interacción segura en el intercambio de datos, debiendo al efecto proporcionar al usuario una certificación para acceder a la red, según lo establecido en el inciso 4º del Art.8 de la ley.

Las funciones de las Autoridades Certificadoras, se encuentran establecidas en el Art. 8-A de la ley, dentro de las cuales tenemos:

- Ejercer la potestad jurídica de otorgar fe pública en el marco del intercambio electrónico de datos.

- Emisión de los certificados digitales.

- Generar el par de llaves, la pública y la privada, verificando el cumplimiento de los requisitos exigidos, la identidad y capacidad del solicitante.

- Llevar un registro público en línea de los certificados, de manera que cualquier persona interesada pueda acceder al directorio de los certificados emitidos y vigentes.

- Tomar medidas para evitar falsificación de los certificados.

La obligación de secreto y reserva de los datos personales de los titulares de los certificados que emitan, se encuentra regulado en el Art. 8-B de la ley. Esta información es considerada de acceso privado, con el objeto de asegurar la confidencialidad, los únicos autorizados a acceder a esta información son la Fiscalía General de la República o un Tribunal competente que con motivos fundados requiera de dicha información.

Dentro de los deberes de las Autoridad Certificadora, enumeradas en el Art. 8-C de la ley tenemos:

- Emitir certificados, implementar sistemas de seguridad, garantizar la protección de la información, garantizar la prestación permanente del servicio, permitir y facilitar la realización de auditorias, elaborar su reglamento y llevar un registro de los certificados emitidos.

Las sanciones que puede imponer el Ministerio de Hacienda a las Autoridad Certificadora se encuentran en el Art. 8-E de la ley. Dependiendo de la naturaleza y la gravedad de la falta, pueden ser:

- Amonestación
- Suspensión de autorización
- Revocación definitiva de autorización para operar.

Las Autoridades Certificadoras ofrecen tres niveles de certificados. Cada nivel o clase de certificado provee servicios específicos en cuanto a funcionalidad y seguridad; los interesados eligen entre estos grupos de servicios el que mas le conviene, según sus necesidades. Cumplidos los requisitos exigidos, se emite el certificado.

**Certificado Nivel 1**

Esta clase de certificados son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indiscutible el nombre del usuario o sus "alias" y su dirección de e-mail con el registro llevado por Verising[93]. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing y Correo electrónico, garantizando la seguridad de sus entornos. En general no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.

Para Certicamara los Certificados Nivel Uno son certificados personales para e-mail, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada.

Son emitidos con el único fin de facilitar la transmisión de información entre partes que utilizan Internet y desean un entorno mas seguro en el envío y recepción de mensajes, básicamente por medio de correo electrónico. La seguridad que proporciona solo está referida a la confirmación del nombre de una persona y la dirección de correo electrónico con la que esa persona ha sido vinculada. Ambos elementos constituyen el único objeto de validación que Certicamara le reconoce.

**Certificado Nivel 2**

Los certificados nivel dos son emitidos a personas físicas y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que esta no difiera de la que surja de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones vía e-mail, transacciones comerciales de bajo riesgo, validación de software y suscripciones on-line.

[93]Verising, es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma electrónica.

Certicamara define a los certificados nivel dos como certificados personales, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada para entornos aplicativos.

Al surgir un proceso de identificación realizado por la entidad solicitante a la que pertenece el titular del certificado, solo poseen la propiedad de autenticar la identidad y facultades de un sujeto determinado en términos de su pertenencia a dicha entidad.

Ya se mencionó anteriormente, de las garantías que otorga Certicamara a sus usuarios, pero tratándose de los certificados digitales niveles 1 y 2, Certicamara no verifica la información suministrada en el requerimiento de certificación por parte de la entidad solicitante o por parte de quien será su titular.

Como consecuencia, Certicamara no es ni será considerada como responsable de la veracidad de cualquiera de los datos contenidos en dicho certificado y quienes pretendan confiar en los certificados digitales niveles 1 y 2 deberán reconocer que sus titulares o la entidad solicitante son responsables por cualquier declaración falsa hecha a Certicamara.

En este sentido, Certicamara no garantiza bajo ninguna circunstancia la no repudiación de las transacciones realizadas por el titular de un certificado nivel 1 y 2, dado que esa circunstancia queda regida exclusivamente por los términos y condiciones que las partes se hayan expresado mutuamente.

**Certificado Nivel 3**

Estos certificados son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, aseguran la identidad del suscriptor; en el caso de las organizaciones, aseguran la existencia y nombre mediante el cotejo de los

registros denunciados en los contenidos de la base de datos independientes. Son utilizados para determinadas aplicaciones de comercio electrónico como Electronic banking y Electronic Data Interchange (EDI).

En Certicamara los certificados nivel tres son certificados personales o jurídicos, con valor legal pleno, cuyos alcances serán explicados en el siguiente capítulo, y son emitidos en un entorno mas seguro y revestidos de ciertos formalismos, no solo respecto del proceso de emisión, ya que para ello resulta indispensable la comparecencia personal del titular ante el agente certificador.

Estas formalidades, realizadas en el contexto del marco jurídico existente, proporcionan una mayor seguridad en las transacciones de Comercio Electrónico y garantizan al mismo tiempo la posibilidad de exigir su cumplimiento mediante los procedimientos jurisdiccionales tradicionales.

Tratándose de los certificados digitales nivel tres, la verificación de la información suministrada en el requerimiento de certificación por parte de quien será su titular, será realizada previa autorización de la Aduana y presentación de los documentos antes mencionados.

De igual forma, la Cámara de Comercio e Industria de El Salvador, ha presentado una fianza de fiel cumplimiento por el servicio de Certificación Electrónica cerrada a favor del Ministerio de Hacienda.

### 4.12 CERTIFICADOS DIGITALES

Pero, ¿cómo sabemos que B y A tienen asignadas las llaves públicas que dicen tener? Pues mediante un mecanismo llamado: Certificado Digital, el cual contiene el nombre de la persona y su llave pública, y está firmado con la llave privada de una Autoridad Certificadora.

Un certificado atestigua la validez de la identidad de un individuo o entidad. Generalmente es emitido por una Autoridad Certificadora, quien al firmar digitalmente une una llave pública con el nombre de un individuo o entidad.

Su propósito es: el permitir la verificación de la premisa que una llave pertenece de hecho a un individuo. El principal inconveniente del uso de claves públicas es el modo de asociación de los pares de llave pública y llave privada con personas físicas. La solución la aportan las Autoridad Certificadora que son entes fiables y ampliamente reconocidos que firman (con conocimiento de causa y asunción de responsabilidad) las claves públicas de las personas, rubricando con su firma su identidad.[94]

A la vista de este esquema de funcionamiento, se plantea un problema evidente de confianza que puede originar varios interrogantes: ¿Cómo tener certeza de que la clave pública de un usuario corresponde realmente a ese individuo y no ha sido falsificada por otro?, ¿Por qué fiarse de esa clave pública antes de confiarle algún secreto?, ¿Quién verifica la identidad del poseedor de la clave pública?

Todas estas preguntas encuentran su respuesta en la figura de los certificados digitales, especie de documentos electrónicos que garantizan la identidad de una persona. Así los certificados digitales contienen de forma estructurada información relevante acerca de usted y de la entidad que lo emitió:

- ✓ El código identificativo único del certificado.

- ✓ La identificación del prestador de servicios de certificación que expide el certificado, es decir, de la autoridad de certificación.

[94] Lopez Oñate “La Certeza del Derecho Digital” Editorial Milano, España, pp. 81-84

- ✓ La firma electrónica del prestador de servicios de certificación que expide el certificado y que da fe de que el certificado expedido es válido y ha sido emitido de acuerdo con sus prácticas de certificación.

- ✓ La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca (información relevante para el uso de que será objeto el certificado).

- ✓ Los datos de verificación de la firma (es decir, la clave pública) que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario (o lo que es lo mismo, su clave privada), de manera que se produce una vinculación exclusiva del interesado con las claves. Esta clave pública es la que permite a su vez, verificar la autenticidad de la firma electrónica.

- ✓ El comienzo y el fin del período de validez del certificado, fuera de los cuales no podrá utilizarse.

- ✓ Los límites de uso del certificado, si se prevén, como por ejemplo compra a través de Internet, acceso a bancos, exclusión de ciertos contratos como préstamos y fianzas, identificación ante servidores en una red local, etc.

- ✓ Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen. De esta forma se controla que con un certificado no puedan efectuarse compras por importe superior a un valor especificado en el mismo.

En síntesis, la función fundamental de los Certificados es: permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica, pertenece realmente a ese usuario, ya que así lo hace constar en el certificado una autoridad que da fe de ello. Representan además, una forma conveniente de hacer llegar la clave pública a otros usuarios que deseen verificar sus firmas. Normalmente, cuando se envía un documento firmado digitalmente, éste siempre se acompaña del certificado del signatario, con el fin de que el destinatario pueda verificar la firma electrónica adjunta.

Estos certificados permitirán a sus titulares realizar una gran cantidad de acciones a través de Internet: acceder por medio de su navegador a sitios Web restringidos, a los cuales les deberá presentar previamente el certificado, cuyos datos serán verificados y en función de los mismos se le permitirá o denegará el acceso; enviar y recibir correo electrónico cifrado y firmado; entrar en intranets corporativas, e incluso a los edificios o instalaciones de la empresa, donde se le pedirá que presente su certificado, posiblemente almacenado en una tarjeta inteligente; firmar software para su uso en Internet, firmar cualquier tipo de documento digital, para uso privado o público; obtener confidencialidad en procesos administrativos o consultas de información sensible en servidores de la Administración; realizar transacciones comerciales seguras con identificación de las partes.[95]

## 4.13 REGISTRO DE CERTIFICADOS

La Agencia Certificadora se define como aquel agente encargado de la autenticación de la identidad de los usuarios de la Autoridad Certificadora (CA). Posteriormente manda la petición del usuario a la Autoridad Certificadora y la clave pública a la Autoridad Registradora.

[95] ídem

La Agencia Certificadora es el intermediario entre los usuarios y la Autoridad Certificadora. La calidad del proceso de autenticación de la Agencia Certificadora determina el nivel de confianza que se tendrá en los certificados.

Una Agencia Certificadora puede ser conceptualizada como un punto de presencia local para la Autoridad Certificadora donde los usuarios pueden aplicar para la obtención de un certificado.

### 4.14 DECLARACIÓN DE PRÁCTICAS DE CERTIFICADOS (CPS)

Las Autoridad Certificadora tienen un conjunto de políticas operativas que describen la implantación y apoyo a las políticas de seguridad condensadas a un detallado documento conocido cono Declaración de Prácticas de Certificación (CPS). Estas políticas incluyen procedimientos de Verificación de Identidad, rango de usurarios a certificar, ciclo de vida de los certificados.

### 4.15 FUNCIONAMIENTO DE LOS CERTIFICADOS

El certificado digital incorpora información sobre el usuario (entre otros datos su clave pública), información que debe ser contrastada por algún tipo de autoridad competente, que dota así de validez al documento acreditativo. En el contexto electrónico, la función básica de una Autoridad de Certificación (AC) o prestador de servicios de certificación (CPS) reside en verificar fehacientemente la identidad de los solicitantes de certificados, crear y emitir a los solicitantes dichos certificados y publicar listas de revocación cuando éstos son inutilizados. Se contempla que cualquier entidad u organización pública o privada se constituya en PSC, fomentando así la libre competencia también en este mercado. Ahora bien, para que una persona física o jurídica se erija en la figura de autoridad de certificación es necesario que cumpla una serie de obligaciones exigibles a todos los prestadores de servicios de certificación que expidan certificados reconocidos, entre las que destacan:

- ✓ La comprobación de la identidad de los solicitantes de los certificados, ya que si esta verificación no se realiza rigurosamente, toda la estructura de certificados y firmas digitales pierde por entero su validez.

- ✓ No almacenar las claves privadas de los usuarios, para preservar su privacidad y evitar la posibilidad de que sean suplantados, ya que hasta cierto punto puede decirse que la identidad digital de un usuario reside en su clave privada.

- ✓ Informar debidamente a los solicitantes acerca de precios y condiciones de utilización de los certificados, precios que estarán regidos por el mercado en régimen de libre competencia.

- ✓ Mantener un registro de todos los certificados emitidos y de su estado de validez.

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

- ✓ Poseer una serie de garantías técnicas que demuestren la factibilidad necesaria de sus servicios, la rapidez y la seguridad en la prestación de los mismos, el empleo de personal cualificado y con la experiencia necesaria para dicha prestación, la utilización de sistemas y productos fiables protegidos contra toda alteración, la toma de medidas contra la falsificación de certificados y el uso de sistemas fiables para almacenarlos.

- ✓ Conservar registrada toda la información y documentación relativa a un certificado reconocido durante un tiempo determinado, con el fin de garantizar

que los certificados puedan ser aportados como prueba en los procesos judiciales que pudieran surgir en relación con el uso de la firma.

Con el tiempo, durante el ejercicio de sus funciones, una autoridad de certificación puede verse fácilmente desbordada si cubre un área geográfica muy extensa o muy poblada, por lo que a menudo delega la labor de verificar la identidad de los solicitantes en las llamadas Agencias De certificación. Las Agencias De certificación pueden abrir multitud de oficinas regionales dispersas por un gran territorio, llegando hasta los usuarios en los sitios más remotos, mientras que la Autoridad Certificadora se limitaría así a certificar a todos los usuarios aceptados por las Agencias De certificación dependientes de ella. Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

## 4.16 RECOMENDACIONES PARA EL USO DE LOS CERTIFICADOS DIGITALES:

**Compromiso de la clave privada del usuario:** si la clave privada cae en manos de un desconocido, éste podría suplantar al usuario y realizar en su nombre todas las acciones a que su certificado le autorice. Suceso más frecuente es que el usuario olvide la contraseña que protege su clave privada, privándose así de su uso. En ambos casos, se debe dar aviso a la Autoridad Certificadora con la mayor brevedad posible para que el certificado sea revocado.

**Compromiso de la clave privada de la Autoridad Certificadora**: un suceso más grave es que se vea comprometida la clave privada de la Autoridad Certificadora, en cuyo caso el desconocido podría suplantar a la propia autoridad de certificación, con consecuencias desastrosas. En cuanto la Autoridad Certificadora lo advirtiera, debería cambiar su clave, quedando invalidados absolutamente

todos los certificados reconocidos emitidos hasta ese momento. Las medidas de seguridad de la empresa de certificación son (deben ser) lo suficientemente estrictas como para que la probabilidad de este suceso sea prácticamente nula.

**Cambio en los datos del certificado**: los usuarios cambian de trabajo, de lugar de residencia, de dirección de correo, etc., motivos que pueden justificar la emisión de un nuevo certificado que refleje verazmente la nueva información personal del titular y la invalidación del certificado antiguo.

**Violación de la política de la Autoridad Certificadora**: si un usuario viola las normas de certificación de la Autoridad Certificadora, ésta puede decidir revocar su certificado.

**Expiración del certificado**: los certificados tienen un tiempo de vida limitado y claramente especificado en sus datos, al final del cual dejan de ser válidos. Esta situación no ocasiona mayores dificultades, y el usuario simplemente deberá solicitar su renovación a la Autoridad Certificadora que se lo emitió.

## 4.17 DISPOSITIVOS DE ALMACENAMIENTO DE CERTIFICADOS DIGITALES:

| Dispositivo de Almacenamiento | | Ventajas | Desventajas |
|---|---|---|---|
| **Chip Card** | Se almacena en una tarjeta inteligente | Se pueden utilizar en cualquier lado. Dispositivo de almacenamiento mas seguro | Es de alto costo ya que se requieren lectoras especiales. La tecnología aún no es accesible para todos los usuarios |
| **Browser** | Se almacena en la computadora del cliente modificando localmente la configuración del Browser del cliente | Es el certificado digital mas barato | Únicamente se puede utilizar desde la computadora a donde se almacenó el certificado digitalmente |

**DISPOSITIVOS DE ALMACENAMIENTO DE CERTIFICADOS DIGITALES:**

| | | | |
|---|---|---|---|
| **Diskette o Disco Duro** | Se almacena en la propia PC y se envía una copia como anexo a los mensajes firmados | Solo puede tener acceso en la PC o con el diskette | Riesgo de robo de la máquina o el diskette |
| **Servidor** | Se almacena en un servidor | El cliente puede tener acceso a través de una clave desde cualquier computadora | Dependencia total de un solo servidor. Cliente se autentica sin certificado |

# CAPITULO V

## 5.1 LA FIRMA ELECTRÓNICA A NIVEL INTERNACIONAL

La firma electrónica tiene muy poco tiempo de haber surgido, debido a la necesidad de un mundo globalizado, en donde las transacciones y la interacción entre individuos son impersonales y sin vínculos físicos, haciendo de la identificación un problema y requerimiento de primera necesidad. Los medios tradicionales de identificación pierden validez en el mundo electrónico, surgiendo así medios digitales de identificación.

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 Acf; 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 Acf que fue aprobada el 30 de julio de 1999. Además el 30 de junio de 2000, se emitió la "Electronic Signatures in Global and National Commerce Acf.

En otros países como es el caso de Italia, el 15 de marzo de 1997, fue publicado el "Reglamento sobre: Acto, Documento y Contrato en forma electrónica". En Argentina el 17 de marzo de 1997, el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la resolución 45/97. En Alemania el 13 de junio de 1997 fue promulgada la Ley sobre Firmas Digitales y el 7 de junio del mismo año, fue publicado su Reglamento. En la Comunidad Económica Europea se emitió el Real Decreto Español sobre Firmas Electrónicas en el mes de septiembre de 1999 y en materia de Firmas Electrónicas en noviembre de 1999. El 16 de diciembre de 1996 se emitió la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

(CNUDIM), la cual es una sugerencia a cada país para eliminar diferencias en la legislación interna y se contribuya a garantizar la seguridad jurídica internacional en el comercio electrónico; y el 5 de julio de 2001 es adoptado por la misma Comisión la Ley Modelo sobre Firmas Electrónicas.

### 5.1.1 EN ESTADOS UNIDOS DE AMERICA

A finales de la década de los setenta, el gobierno de los Estados Unidos publicó el de Estandar de Datos Encriptados para sus comunicaciones de datos sensibles pero no clasificados. El 16 de abril de 1993, el gobierno de los EE.UU. anunció una nueva iniciativa criptográfica encaminada a proporcionar a los civiles, un alto nivel de seguridad en las comunicaciones: proyecto Clipper. Esta iniciativa está basada en dos elementos fundamentales:

- ✓ Un chip cifrador a prueba de cualquier tipo de análisis o manipulación y
- ✓ Un sistema para compartir las claves secretas que, en determinadas circunstancias, otorgaría el acceso a la clave maestra de cada chip y que permite conocer las comunicaciones cifradas por él.

En EE.UU. es donde más avanzada está la legislación sobre firma electrónica, aunque el proyecto de estandarización del NIST[96] no lo consiga. El NIST ha introducido dentro del proyecto Capstone, el DSS (Digital Signature Standard) como estándar de firma, si bien todavía el gobierno americano no ha asumido como estándar su utilización. El NIST se ha pronunciado a favor de la equiparación de la firma manuscrita y la electrónica.

La ley de referencia de la firma electrónica, para los legisladores de los Estados Unidos, es la ABA (American Bar Association), Digital Signature Guidelines, de 1 de agosto de 1996.

[96] Instituto Nacional de Ciencia y Tecnología: www.nist.gov

El valor probatorio de la firma ha sido ya admitido en Utah, primer estado en legislar sobre firma digital. La firma digital de Utah (de 27 de febrero de 1995, modificado en 1996) se basa en un "Criptosistema Asimétrico" definido como: un algoritmo que proporciona una pareja de claves segura.

Sus objetivos son, facilitar el comercio por medio de mensajes electrónicos fiables, minimizar las incidencias de la falsificación de firmas digitales y el fraude en el comercio electrónico.

La firma digital es una transformación de un mensaje utilizando un criptosistema asimétrico, de tal forma que una persona que tenga el mensaje cifrado y la clave pública de quien lo firmó, puede determinar con precisión el mensaje en claro y si se cifró usando la clave privada que corresponde a la pública del firmante.

Esta ley establece la presunción, de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen ciertas existencias; una es que la firma digital sea verificada por referencia a una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia.

El Estado de Utah ha redactado un proyecto de ley (The Act on Electronic Notarization) en 1997.

California define la firma digital como la “creación por ordenador de un identificador electrónico que incluye todas las características de una firma válida, aceptable, como:

- Única
- Capaz de comprobarse
- Bajo un solo control

- Enlazándose con los datos de tal manera que si se cambian los datos se invalide la firma

- Adoptada al menos como un estándar por dos de las organizaciones siguientes:
  - The International Telecommunication Unión.
  - The American National Standards Institute.
  - The Internet Activities Board.
  - The National Institute of Science and Technology.
  - The International Standards Organization."

Podemos hacer referencia también a:

- ABA, Resolution conceming the CyberNotary: an International computer-transaction specialist, de 2 de agosto de 1994.

- The Electronic Signature Act Florida, de mayo de 1996 que reconoce la equivalencia probatoria de la firma digital con la firma manual. En esta ley se usa el término de "international notar/' en vez del "cybernotary" utilizado en otras leyes de EE.UU.

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

- The Massachusetts Electronic Records and Signatures Act, de 1996, que acoge todo mecanismo capaz de proporcionar las funciones de la firma manuscrita sin ceñirse a un tipo concreto de tecnología.

**NCCSL**

- El 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, elaboró la "Uniform Electronic Transactions Act" (UETA), la cual se aprobó el 30 de julio de 1999.
- El 4 de agosto del 2000 se aprobó la "Uniform Computer Information Transactions Act" (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana.

**PRESIDENCIA**

- El 30 de junio el 2000 se emite la "Electronic Signatures in Global and Nacional Commerce Act" (E-Sign Act.) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

Conseguir una ley que impere en la totalidad del país de los 114 millones de internautas está resultando una tarea más que ardua.

El 9 de noviembre del 2001 el Congreso de los EEUU, aprobó una legislación para sustituir la firma convencional por la digital en determinados documentos. Aunque la votación pública resultó llamativamente positiva para la firma electrónica (356/66), todavía queda mucho camino por delante. De entrada la oposición ha solicitado que se repita la votación, pero que esta vez sea secreta. Aún repitiéndose el resultado, es muy probable que la Casa Blanca vete la propuesta alegando que agrede los derechos de los ciudadanos, y su paso por el Senado puede transformar completamente la propuesta de ley.[97]

[97] Instituto Nacional de Ciencia y Tecnología: www.nist.gov

## 5.2 EN LATINOAMÉRICA

### 5.2.1 MÉXICO.

Respecto de México los principales antecedentes legislativos se dan en el Código de Comercio de 1884 en el que existen disposiciones relativas al telégrafo como medio de comunicación; en el Código Civil de 1928 hace referencia en diversas disposiciones al teléfono; en las Leyes Bancarias de 1990 incorpora los medios telemáticos; la Ley de Protección Federal al Consumidor de 1992 protege a los consumidores de las ventas a distancia y tele marketing, es decir ventas por medio de medios de comunicación masiva como son el radio y televisión; dentro de las diversas Leyes Fiscales de 1998 igualmente se prevén las declaraciones y pagos en formato electrónico, además de diversos esfuerzos gubernamentales.

La legislación existente hasta el año de 1999, requería para la validez del acto o contrato, del soporte de la forma escrita y la firma autógrafa para vincular a las partes en forma obligatoria y la necesidad de modernizar la legislación mexicana para el reconocimiento jurídico de transacciones por Internet. En abril de 1999, el Partido Acción Nacional presentó la iniciativa del texto de la Ley Modelo de UNCITRAL y en marzo de 2000 el Partido Revolucionario Institucional presenta la iniciativa de texto simplificado y aumentado con Protección al Consumidor.

Después de varios meses de análisis de proyectos, y ante la consideración generalizada sobre la conveniencia de adecuar la legislación mexicana para dar seguridad jurídica en el uso de medios electrónicos, se aprobó en México el Decreto de fecha 29 de abril de 2000 mediante el cual se reformó y se adicionaron disposiciones al Código Civil Federal, Código Federal de Procedimientos Civiles, Código de Comercio y a la Ley Federal de Protección al Consumidor para establecer el esquema jurídico para brindar mayor certeza a las operaciones vía electrónica o digital.

Ante estos antecedentes, la doctrina ha definido a la firma como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto. También la podemos definir como el conjunto de letras y signos entrelazados, que identifican a la persona que la estampa con un documento o texto. Respecto de la firma electrónica no existe todavía un acuerdo al respecto, algunos la consideran un sello y otros hacemos un distingo entre firma electrónica y firma electrónica avanzada, partiendo de la base de la garantía de integridad, atribución y accesibilidad que pudiere darse:

**a)** FIRMA ELECTRÓNICA

A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar y/o vincular al firmante en relación con el mensaje de datos, en forma equivalente a la firma manuscrita.

**b)** FIRMA ELECTRÓNICA AVANZADA

A la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control, conocida también como firma digital, que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier modificación ulterior de éste.

### 5.2.2 ARGENTINA[98]

En marzo de 1999 se encargó a un grupo de juristas (Comisión creada por Decreto 685/95) la redacción de un Proyecto de Código Civil que también abarcase las materias electrónico comerciales, en el cual se prevén importantes modificaciones en el tratamiento de los instrumentos. Se mantiene la regla de libertad de formas y se prevé la forma convenida que es obligatoria para las partes bajo pena de invalidez del negocio jurídico. Se reconocen los instrumentos

[98] http://snts1.jus.gov.ar/minis/Nuevo/ProyectoCodigoCivil.htm

públicos, los instrumentos privados y los instrumentos particulares que son los no firmados.

Lo relevante es:

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

- Se define la firma y se considera satisfecho 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. En este sentido el Código se abre a la realidad abrumadora de los documentos electrónicos, aunque con fórmulas abiertas y flexibles y sin vinculación a la tecnología actual, de modo de evitar su rápido envejecimiento que se produciría por la previsible permanente superación de esas tecnologías.

En las escrituras públicas se incorporan dos reglas novedosas. La primera relativa a la justificación de la identidad, que sustituye a la fe de conocimiento; se prevé incluso la posibilidad de insertar la impresión digital del compareciente no conocido por el notario.
La segunda es la reglamentación de las actas, a las que sólo se asigna valor probatorio cuando son protocolares.

En materia de instrumentos privados, se regula expresamente el valor probatorio del documento electrónico, que se vincula a los usos, a las relaciones preexistentes de las partes y a la confiabilidad de los métodos usados para asegurar la inalterabilidad del texto. Cabe apuntar que en cuanto a la noción de

firma y de valor probatorio, se han tenido especialmente en consideración la ley modelo de comercio electrónico elaborada por UNCITRAL, el Código de Québec y las tentativas de reforma del Código Civil francés en materia de prueba.

La contabilidad y estados contables tienen un tratamiento con numerosas novedades. En esta materia se siguen los Proyectos de Código Único de 1987 y los de 1993 (el de la Comisión Federal y el de la Comisión designada por decreto 468/92). El sistema propuesto permite al interesado llevar el sistema de registros mediante métodos mecánicos, electrónicos o libros.

### 5.2.3 COLOMBIA[99]

Ley 527 de 1999 (Agosto 18). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.

### 5.2.4 CHILE[100]

El 10 de junio de 1999 el presidente Eduardo Freí, presentó el decreto 81 que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado (ha sido aprobado por la Cámara de Diputados del Congreso chileno, y debe ser enviado para su segundo trámite constitucional al Senado de la República) que nada tiene que ver con el comercio electrónico, sino que se relaciona sólo con el uso de firmas y documentos digitales o electrónicos al interior de la Administración del Estado, obedece a uno de los compromisos adoptados por una Comisión Presidencial de Nuevas Tecnologías que sesionó durante 1998, en orden a dotar a los órganos estatales del marco legal que permita el uso de la informática y de las telecomunicaciones en reemplazo de sus procedimientos manuales,

[99] *Sitio en internet de la Corte Constitucional de Colombia*
[100] Renato Jijena Leiva. Universidad de Chile; Federación Iberoamericana de Asociaciones de Informática y Derecho (FIADI) Firma Digital y Entidades Certificadoras. Regulación Legal en la Administración Pública Chilena

específicamente en lo relacionado con el uso de firmas y de documentos digitales al interior de la Administración del Estado y no en las eventuales relaciones con los administrados.

El 9 de agosto del 2000 inició, como complemento, un proyecto de ley que regula la firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento voluntario de acreditación de prestadores de servicio de certificación, para su uso en actos o contratos celebrados por medio de documentos electrónicos a través de medios electrónicos de comunicación (retomando algunos conceptos del decreto anotado anteriormente). En el cual se define:

**a)** CERTIFICADO DE FIRMA ELECTRÓNICA: certificación electrónica que da fe sobre los datos referidos a una firma electrónica simple o avanzada;

**b)** CERTIFICADOR: entidad prestadora de servicios de certificación de firmas electrónicas;

**c)** DOCUMENTO ELECTRÓNICO: toda representación electrónica que dé testimonio de un hecho, una imagen o una idea;

**d)** ENTIDAD ACREDITADORA: la Subsecretaría de Economía, Fomento y Reconstrucción.

**e)** FIRMA ELECTRÓNICA AVANZADA**:** es aquélla creada usando medios que el titular mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, y permita que sea detectable cualquier modificación ulterior de éstos, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento y la integridad del mismo;

**f)** FIRMA ELECTRÓNICA SIMPLE**:** es aquélla que no reúne alguno de los elementos que definen a la firma electrónica avanzada;

**g)** FIRMA ELECTRÓNICA**:** cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar solo formalmente a su autor;

**h)** USUARIO O TITULAR**:** persona que utiliza bajo su exclusivo control un certificado de firma electrónica.

### 5.2.5 ECUADOR[101]

2001. En marzo del 2001 se presentó un Proyecto de Ley de Comercio Electrónico y firmas digitales, en términos muy similares a la Chilena, utilizando el modelo mexicano.

### 5.2.6 PANAMÁ[102]

Ley número 43, del 31 de julio del 2001, se expidió la 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, definiendo:

**a)** CERTIFICADO*.* Manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas electrónicas o la integridad de un mensaje.

**b)** DESTINATARIO*.* Persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a ese mensaje.

[101] Dr. José Luis Barzallo. Quito - Ecuador, sbarzal@uio.satnet.net
[102] Publicada en la Gaceta Oficial No. 24.359 de 3 de agosto de 2001

**c)** DOCUMENTO ELECTRÓNICO. Toda representación electrónica que da testimonio de un hecho, una imagen o una idea.

**d)** ENTIDAD DE CERTIFICACIÓN**.** 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.

**e)** FIRMA ELECTRÓNICA. Todo sonido, símbolo o proceso electrónico vinculado lógica y asociadamente 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.

**f)** INICIADOR. Toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado, para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a ese mensaje.

**g)** INTERMEDIARIO. Toda persona que, actuando por cuenta de otra, envíe, reciba o archive un mensaje o preste algún otro servicio con respecto a él.

**h)** MENSAJE DE DATOS. Información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

**i)** REPOSITORIO. Sistema de información utilizado para guardar y recuperar certificados u otro tipo de información relevante para la expedición de éstos.

**j)** REVOCAR UN CERTIFICADO. Finalizar definitivamente el periodo de validez de un certificado, desde una fecha específica en adelante.

**k)** SISTEMA DE INFORMACIÓN. Todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

**l)** SUSCRIPTOR. Persona que contrata con una entidad de certificación la expedición de un certificado, para que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma electrónica.

**m)** SUSPENDER UN CERTIFICADO. Interrumpir temporalmente el periodo operacional de un certificado, desde una fecha en adelante.

### 5.2.7 PERÚ[103]

El 9 de agosto de 1999 se presentó el proyecto de ley que regula la contratación electrónica[104], el cual fue dado a conocer en Washington DC en el seminario denominado *"RESPONDING TO THE LEGAL OBSTACLES TO ELECTRONIC COMMERCE IN LATÍN AMERICA,* organizado por *National Law Center ínter American Free Trade. The organization of American States Business Software Alliance* (Septiembre 29- Octubre 1 , 1999), tiene por objeto regular la utilización de la firma electrónica, otorgándole plena validez y eficacia jurídica equiparada al uso de una firma manuscrita u otra análoga que conlleve

[103] Dictamen de la Comisión de Reforma de Códigos recaído sobre el proyecto de ley 5070-99 CR que regula las firmas electrónicas, suscrito por el congresista Jorge Muñiz Ziches.
[104] proyecto de ley 5070-99 CR

manifestación de voluntad. El cual se fundamenta en la legislación colombiana, argentina, chilena y mexicana y fue aprobado por unanimidad por la Comisión de Reforma de Códigos.

### 5.2.8 VENEZUELA[105]

El 26 de abril del 2000 se presentó un proyecto de LEY ORGÁNICA DE TECNOLOGÍAS DE INFORMACIÓN, tiene por objeto promover y desarrollar el uso intensivo de las tecnologías de información en la sociedad, y regular el régimen jurídico de la función y el servicio público del sector de tecnologías de información estableciendo los principios orientadores y regulando los procesos de formación de políticas, normas, estrategias, planes y acciones tecnológicas del Estado a objeto de establecer la Infraestructura Nacional de Tecnologías de Información, entendiendo por ésta el conjunto de servicios y productos del sector de tecnologías de información, incluyendo aquellos que soportan el intercambio y difusión de información en la Nación a través de redes de transmisión de datos de carácter público o privado, pero de uso público, que se encuentren conectadas entre si y a su vez puedan conectarse con entidades similares en el exterior. No considera el Comercio Electrónico, pero como en el caso de Chile establece lineamientos e instituciones para regular el uso de la firma digital y los documentos electrónicos en la Administración del Estado.

## 5.3 EN EUROPA

### 5.3.1 ESPAÑA[106]

La legislación actual y la jurisprudencia, son suficientemente amplias para acoger bajo el concepto de firma y de escrito a la firma digital y a cualquier otro tipo de firma. Cierto es que por razones de seguridad y para ofrecer mayor confianza en los usuarios y jueces que a la postre deben juzgar sobre la firma digital,

[105] Sitio en internet del gobierno de Venezuela. Texto en discusión elaborado con la participación de los sectores académico, gubernamental y economía privada
[106] Ley 59, de firma electrónica http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343..pdf

El artículo 3 del RD. 2402/1985, de 18 de diciembre, al regular los requisitos mínimos de las facturas, no exige que se firmen. Creemos no existe inconveniente alguno en admitir la posibilidad de una firma electrónica.

La Circular del Banco de España 8/88 de 14 de Junio creando el reglamento del Sistema Nacional de compensación electrónica, se convirtió en pionera y marcó un hito para la protección y seguridad necesaria en la identificación para el acceso a la información, al indicar que la información se cifrará, para que las entidades introduzcan un dato de autentificación con la información de cada comunicación, a lo que se le reconoce a este método el mismo valor que el que posee un escrito firmado por personas con poder bastante.

El artículo 45 de la Ley 30/1992 de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común incorporó el empleo y aplicación de los medios electrónicos en la actuación administrativa, de cara a los ciudadanos. Para su regulación, el Real Decreto 263/1996 de 16 de febrero, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación legal de la "firma electrónica".

Es de hacer notar que la circular 3/2001 del Banco de España que modifica a la circular 8/90 regula, por primera vez, algunos aspectos jurídicos contractuales de contratos bancarios realizados por Internet (incluyendo el concepto *soporte electrónico duradero* e *informaciones electrónicas)*

Tras un Real Decreto del 17 de septiembre de 1999, en el que se reconoció el uso de la firma electrónica, su eficacia jurídica y la prestación al público de servicios de certificación. El 21 de octubre se convalidó La Ley sobre Firma Digital con los votos a favor de PP (impulsor del proyecto) CIU, PNV y Coalición

Canaria, y la oposición de PSOE y Grupo Mixto que no veían la urgencia de esta norma ni la necesidad de aprobarla como Real Decreto Ley. El 17 de noviembre, durante las jornadas de Comercio electrónico de *FECEMD Federación de Comercio electrónico y Marketing Directo),* el Secretario General de Comunicaciones anunció que casi toda la Ley sobre Firma Electrónica es aplicable directamente, pero que aún resta un pequeño porcentaje (en el que se incluye la acreditación de las entidades certificadoras) que exige un breve reglamento que se está ultimando.

Aquellos que se oponen a la regulación de la firma electrónica alegan que es precipitado e imprudente tomar medidas tan pronto, porque si la iniciativa comunitaria va por otro camino puede quedar desfasada. Y realmente sería muy peligroso crear barreras internas para el comercio electrónico (deberíamos haber aprendido de la experiencia con los ferrocarriles de vía ancha y vía estrecha).

No parece que vayan a producirse demasiados conflictos. El 26 de octubre, tras una serie de difíciles negociaciones sobre los niveles de seguridad, el Parlamento Europeo aprobó una ley comunitaria que establece un marco común para la firma electrónica, y los ministros de la CMT[107](Comisión del Mercado de las Telecomunicaciones) son los encargados de velar por ello.

Actualmente en España se está trabajando en el ANTEPROYECTO DE LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (18 de enero del 2002) que regula ciertos aspectos jurídicos de los servicios de la sociedad de la información y de la contratación por vía electrónica, como las obligaciones de los prestadores de servicios que actúan como intermediarios en la transmisión de contenidos por la Red, las comunicaciones comerciales, la información previa y posterior a la celebración de

[107] http://www.cmt.es

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. Incorporando novedades importantes como la necesidad de constancia registral del Nombre de Dominio, ciertas obligaciones en relación con los contenidos en Internet, régimen de responsabilidad de los prestadores de servicios de información y certificación, impulso a la elaboración y aplicación de Códigos de Conducta, regulación de comunicaciones comerciales y contratación por vía electrónica, solución judicial y extrajudicial de conflictos (procurando fomentar la solución extrajudicial de litigios vía arbitraje), supervisión y control, infracciones y sanciones, así como reformas que pemitan la informatización de los Registros Públicos.

Parece garantizado que dentro de la UE la firma será compatible, pero es deseable que también lo sea con otros países con los que también se llevan a cabo transacciones comerciales EEUU, Latinoamérica... y eso todavía no está tan claro.

### 5.3.2 ALEMANIA[108]

La ley de firma digital regula los certificados de las claves y la autoridad certificadora. Permite el seudónimo, pero prevé su identificación real por orden judicial. A la firma electrónica se la define como sello digital, con una clave privada asociada a la clave pública certificada por un certificador.

La Ley de 19 de septiembre de 1.996 es el primer proyecto de ley de firma digital en Europa. (Entra en vigor el 1 de noviembre de 1997).

[108] - Ley de firma electrónica http://www.bundesnetzagentur.de/media/archive/3612.pdf
Reglamento de firma electrónica http://www.bundesnetzagentur.de/media/archive/3613.pdf

### 5.3.3 ITALIA[109]

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

El reglamento aprobado por el Consejo de Ministros el 31 de octubre de 1997, criterio y modalidades para la creación, archivo y transmisión de documentos con instrumentos informáticos y telemáticos de acuerdo con el art. 15 inciso dos de la Ley

Esta basada esta normativa en soluciones extranjeras y supranacionales.

### 5.3.4 REINO UNIDO[110]

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

## 5.4 EN LOS PAÍSES BAJOS

Se ha creado un organismo interministerial encargado del estudio de la firma digital. En Dinamarca, Suiza y Bélgica Preparan proyectos de ley sobre firma digital.

### 5.4.1 SUECIA[111]

Organizó una audiencia pública sobre la firma digital en 1997.

[109] Decreto legislativo n. 10, , de firma electrónica http://protocollo.gov.it/normativa/dlgs10_02.asp

[110] Reglamento de firma electrónica http://www.opsi.gov.uk/SI/si2002/20020318.htm

[111] Ley 832, de firma electrónica reconocida http://www.sweden.gov.se/content/1/c6/02/72/93/569fc933.pdf

### 5.4.2 EN LA COMUNIDAD EUROPEA[112]

Unión Europea. Directiva 2000/31/CE del parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de información, en particular el Comercio Electrónico en el mercado interior (Directiva sobre el Comercio Electrónico).

Unión Europea. Directiva del Parlamento Europeo y del Consejo por el que se establece un marco comunitario para la Firma Electrónica (1999)

El artículo 6 del Acuerdo EDI de la Comisión de la Comunidades Europeas, que determina la necesidad de garantía de origen del documento electrónico, no regula la firma electrónica.

No obstante *Perales Viscasillas* cree que no existe inconveniente alguno en admitir la posibilidad de una firma electrónica apoyada en las siguientes circunstancias:

- ✓ La fiabilidad de la firma electrónica es superior a la de la firma manuscrita.
- ✓ La equiparación en el ámbito comercial internacional de la firma electrónica y la firma Manuscrita.

En el contexto de las transacciones *EDI* es habitual la utilización de la conocida como "firma digital" que se basa en "algoritmos simétricos" en los que ambas partes conocen la misma clave o en "algoritmos asimétricos" en los que, por el contrario, cada contratante tiene una clave diferente.

En el mismo sentido *Isabel Hernando,* refiriéndose a los contratos-tipo en *EDI* indica que si los mensajes *EDI* se transmiten mediante procedimientos de

[112] Union Europea. Directiva 2000/31CE del Parlamento Europeo y del Consejo del 8 de junio de2000relativa a determinar los aspectos jurídicos de los servicios de la sociedad de información en particular el Comercio Electrónico en el mercado interior (Directiva sobre el Comercio Electrónico).

autentificación como una firma digital, estos mensajes tendrán entre las partes contratantes el mismo valor probatorio que el acordado a un documento escrito firmado.

La Comisión Europea, ha financiado numerosos proyectos *(INFOSEC, SPRI,* etc.) cuyo objetivo es la investigación de los aspectos técnicos, legales y económicos de la firma digital.
La Comisión Europea hizo pública en octubre de 1997 una Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones titulada "Iniciativa Europea de Comercio Electrónico", con un subtítulo de "Hacia un Marco Europeo para la Firma Digital y el Cifrado".

En el segundo trimestre del 1998 empezaron a encauzar las propuestas para nuevas medidas, una de las cuales podría ser la elaboración de una Directiva de firma digital.
Lo que pretende la Comisión Europea[113] es encontrar un reconocimiento legal común en Europa de la firma digital, con el objeto de armonizar las diferentes legislaciones, para que ésta tenga carta de naturaleza legal ante tribunales en materia penal, civil y mercantil, a efectos de prueba, apercibimiento y autenticidad. A efectos de dar cumplimiento a esta previsión, se expidió a finales de 1998 un borrador de propuesta de directiva sobre firma electrónica y servicios relacionados. Pese a la seguridad ofrecida por la firma digital, el borrador de propuesta de directiva regula la firma electrónica en general, y no sólo la firma digital en particular, en un intento de abarcar otras firmas electrónicas, basadas en técnicas distintas de la criptografía asimétrica. Esta tendencia a la neutralidad tecnológica se ha acentuado a medida que se han ido sucediendo las distintas versiones del borrador de directiva, como pone de manifiesto el hecho de que la

[113] Union Europea. Directiva 2000/31CE del Parlamento Europeo y del Consejo del 8 de junio de2000relativa a determinar los aspectos jurídicos de los servicios de la sociedad de información en particular el Comercio Electrónico en el mercado interior (Directiva sobre el Comercio Electrónico

versión actual defina única y exclusivamente la firma electrónica (art. 2.1), mientras que en el primer borrador existía también una definición de firma digital, en el art. 2.2.; y del par de claves, pública y privada, en los art. 2.4 y 2.5. únicamente al establecer el concepto de elemento de creación de firma (definido, en el art. 2.3, como aquel dato único, como códigos o claves criptográficas privadas, o un elemento físico configurado de forma única, el cual es usado por el firmante para crear una firma electrónica) y elemento de verificación de firma (definido, en el art. 2.4, como aquel dato único, como códigos o claves criptográficas públicas, o un elemento físico configurado de forma única, el cual es usado para verificar una firma electrónica) existe una referencia a la criptografía asimétrica. Esta neutralidad es seguramente conveniente, para dejar abiertas las puertas a desarrollos tecnológicos futuros. Pero, por otra parte, llevada a ese extremo, deja sin resolver, porque no son siquiera abordados, muchos de los problemas planteados actualmente por las firmas digitales, únicas firmas electrónicas seguras hoy día.

Para conseguir una coherencia europea se deberá, sin duda, pasar por el establecimiento de una política europea de control armónica con otras potencias económicas como EE.UU., Canadá y Japón.

### 5.6 ORGANISMOS Y ASOCIACIONES INTERNACIONALES

1. COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL **(UNCITRAL)**
2. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES **(UIT**)
3. ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO **(OCDE)**
4. CÁMARA DE COMERCIO INTERNACIONAL **(CCI)**
5. ORGANIZACIÓN DE NORMAS INTERNACIONALES **(ISO/IEC**)

6. CENTRO DE LAS NACIONES UNIDAS PARA LA FACILITACIÓN DEL COMERCIO Y NEGOCIOS ELECTRÓNICOS (**NU-CEFACT)**
7. UNIÓN UNIVERSAL DE SERVICIOS POSTALES **(UPU)**
8. ORGANIZACIÓN MUNDIAL DE ADUANAS **(OMA)**
9. COOPERACIÓN ECONÓMICA ASIA -PACÍFICO **(APEC)**
10. ÁREA DE LIBRE COMERCIO DE LAS AMERICAS **(ALCA)**
11. BARRA AMERICANA DE ABOGADOS **(ABA)** (AMERICAN BAR ASSOCIATION)
12. GLOBAL BUSINESS DIALOG ON ELECTRONIC COMMERCE **(GBDE)**

### 5.6.1 COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (UNCITRAL)

Intemacionalmente, la UNCITRAL ha completado trabajos sobre modelos de ley que soporta el uso comercial de contratos internacionales en comercio electrónico. Estos modelos de ley, establecen reglas y normas que validan y reconocen los contratos celebrados por medios electrónicos, establecen reglas para la formación de los contratos y su desempeño, definen las características para un escrito electrónico válido o un documento original, proporcionan los elementos funcionales para la aceptación de las firmas electrónicas para propósitos legales y comerciales y apoyan la admisión de pruebas técnica en los tribunales y procedimientos de arbitraje.

Distintos gobiernos han adoptado los Lineamientos de las leyes modelo en diferentes formas y alcances como principios para definir un marco internacional uniforme para el comercio electrónico.

De acuerdo con la UNCITRAL, en la medida de lo posible, los siguientes principios deben guiar el diseño de reglas que gobiernen las transacciones electrónicas internacionales:

Las partes deben ser libres de elegir la relación contractual, entre ellas, la que mejor les convenga;
Las reglas deben ser tecnológicamente neutras (no deben requerir ni asumir una tecnología en particular);
Las reglas deben prever futuros desarrollos tecnológicos (no deben limitar o impedir el uso o desarrollo de nuevas tecnologías);
Las reglas existentes deben ser modificadas y adoptar leyes nuevas solo en la medida necesaria o substancialmente deseable para soportar el uso de tecnologías electrónicas; y

El proceso debe involucrar tanto a los sectores comerciales de alta tecnología como a los negocios que aún no están en línea.

#### 5.6.1.1 LEY MODELO DE UNCITRAL SOBRE COMERCIO ELECTRÓNICO

Esta Ley Modelo fue adoptada en 1996 y tiene por objeto facilitar el uso de medios modernos de comunicación y de almacenamiento de información, por ejemplo el intercambio electrónico de datos (EDI), el correo electrónico y la telecopia, con o sin soporte como sería el Internet. Se basa en el establecimiento de un equivalente funcional de conceptos conocidos en el tráfico que se opera sobre papel, como serían los conceptos "escrito", "firma" y "original". La Ley Modelo proporciona los criterios para apreciar el valor jurídico de los mensajes electrónicos y resulta muy importante para aumentar el uso de las comunicaciones que se operan sin el uso del papel. Como complemento de las normas generales, la Ley Modelo contiene también normas para el comercio electrónico en áreas especiales, como sería el transporte de mercancías. Adicionalmente y con el propósito de guiar y ayudar a los poderes ejecutivos, legislativo y judicial de los países, la UNCITRAL ha elaborado además una Guía para la Incorporación de la Ley Modelo de la UNCITRAL sobre Comercio Electrónico al derecho interno.

### 5.6.1.2 LEY MODELO DE UNCITRAL PARA LAS FIRMAS ELECTRÓNICAS

El creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas (a las que puede denominarse en general "firmas electrónicas"). El riesgo de que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la interoperabilidad jurídica y técnica.

Partiendo de los principios fundamentales que subyacen en el artículo 7 de la Ley Modelo de la UNCITRAL sobre Comercio Electrónico, con respecto al cumplimiento de la función de la firma en el ámbito electrónico, la finalidad de la Ley Modelo para las Firmas Electrónicas es:

- Ayudar a los Estados a establecer un marco legislativo moderno, armonizado y equitativo para abordar de manera más eficaz las cuestiones relativas a las firmas electrónicas.

- Ofrece normas prácticas para comprobar la fiabilidad técnica de las firmas electrónicas.

- Brindar fiabilidad técnica y la eficacia jurídica que cabe esperar de una determinada firma electrónica.

La Ley Modelo para las Firmas Electrónicas, supone una contribución importante a la Ley Modelo de la UNCITRAL sobre Comercio Electrónico, al adoptar un criterio

conforme al cual puede determinarse previamente (o evaluarse con anterioridad a su empleo) la eficacia jurídica de una determinada técnica de creación de una firma electrónica.

Así pues, la Ley Modelo para las Firmas Electrónicas, tiene como finalidad mejorar el entendimiento de las firmas electrónicas y la seguridad de que puede confiarse en determinadas técnicas de creación de firma electrónica en operaciones de importancia jurídica.

Además, al establecer con la flexibilidad conveniente una serie de normas básicas de conducta para las diversas partes que puedan participar en el empleo de firmas electrónicas (es decir, firmantes, terceros que actúen confiando en el certificado y terceros prestadores de servicios), la Ley Modelo para las Firmas Electrónicas puede ayudar a configurar prácticas comerciales más armoniosas en el ciberespacio.

Entre los objetivos[114] de la Ley Modelo para las Firmas Electrónicas, entre los que figuran:

Permitir o facilitar el empleo de firmas electrónicas y

Conceder igualdad de trato a los usuarios de documentación consignada sobre papel como a los usuarios de información consignada en soporte informático.

La Ley Modelo de Uncitral sobre firma electrónica de 2001 define firma electrónica como: *"los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante*

[114] Son fundamentales para promover la economía y la eficacia del comercio internacional. Al incorporar a su derecho interno los procedimientos que se recogen en la Ley Modelo para las Firmas Electrónicas (y la Ley Modelo de la UNCITRAL sobre Comercio Electrónico) para todo supuesto en que las partes opten por emplear medios electrónicos de comunicación, el Estado promulgante creará un entorno jurídico neutro para todo medio técnicamente viable de comunicación comercial.

*aprueba la información contenida en el mensaje de datos". Y distingue la firma electrónica "fiable"*, como aquella en la que:

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; y

Es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

### 5.6.2 UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT)

A. Iniciativa de Comercio Electrónico para Países en Desarrollo.

Desde el lanzamiento de la iniciativa especial de desarrollo de la UIT Electronic Commerce for Developing Countríes, EC-DC, (Comercio Electrónico para Países en Desarrollo) en marzo de 1998 para promover proyectos de comercio electrónico, el apoyo y participación de más de 100 países en desarrollo y diversos socios industriales, ha transformado esta iniciativa en un despliegue mundial de transacciones electrónicas utilizando las tecnologías de Infraestructura de Llave Pública (PKI por sus siglas en Inglés) como la tecnología principal.

La tecnología PKI, simplifica problemas administrativos clave asociados con las soluciones criptográficas simétricas (la misma clave encripta y desencripta), utilizando los algoritmos de claves asimétricas (una clave encripta y otra desencripta) esta tecnología permite soportar la confidencialidad, integridad de los datos y la autentificación de la entidad origen del mensaje. Las aplicaciones que

requieren estándares basados en seguridad (correo electrónico, Internet, seguridad IP y transacciones comerciales), han sido mejoradas para obtener total ventaja de esta tecnología.

Un certificado digital, es un conjunto de datos que confirma la relación de una llave o clave pública al nombre y otros atributos de un individuo u otra entidad. Los formatos mayor aceptados son el estándar X.509 versión 3 de la Unión Internacional de Telecomunicaciones y las claves PGP (Pretty Good Privacy).

Las bases de la seguridad dependen de la fuerza criptográfica de la relación de las claves (privada y pública) en el certificado, la implantación adecuada de las aplicaciones de PKI y el control de la llave o clave privada utilizada para firmar el certificado por su usuario o entidad final.

Con la posibilidad de conjuntar diversas empresas lideres en tecnologías de información y comunicaciones para trabajar dentro del marco de la estrategia de la UIT, una tecnología PKI operacional junto con aplicaciones[115] son funcionales y actualmente en uso en más de 100 países en desarrollo. Por primera vez, diversos países en desarrollo están activamente involucrados en el despliegue de servicios dirigidos a construir la infraestructura de seguridad y confianza (firmas y certificación digital) para diferentes sectores como salud, negocios, educación y gobierno.

[115] (comunicaciones seguras, mercados electrónicos seguros y tecnologías cohesivas basadas en XML)

### 5.6.3 ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO {OCDE)[116]

El comercio electrónico es un elemento central en la visión de la OCDE en que nuestro mundo sistematizado se apoya para el crecimiento económico sustentable, creando más y mejores trabajos, expandiendo el comercio mundial y mejorando las condiciones sociales. El análisis de la OCDE ha permitido una amplia política de reflexión basada en el establecimiento de diversos elementos que pueden proporcionar un ambiente más favorable para el comercio electrónico.

Este comercio es intrínsicamente transfronterizo y el éxito de su desarrollo depende en gran medida en soluciones transfronterizas basadas en políticas de coordinación entre países y entre los habitantes interesados de distritos electorales. Han surgido recomendaciones específicas en áreas como telecomunicaciones, infraestructura y servicios, tributación, protección al consumidor, sistemas de seguridad y privacidad y protección de datos.

En el área de tributación, los gobiernos continúan tratando de incrementar ingresos sin distorsionar alternativas económicas y tecnológicas. El Marco sobre Condiciones de Tributación de 1998 proporciona principios que guiarán a los gobiernos en su aproximación al comercio electrónico, señalando que deberán ser considerados en forma similar al comercio tradicional y destacando la necesidad de evitar cualquier trato discriminatorio.

Tener un mayor alcance a países no-miembros es ahora una prioridad importante en todas las áreas de la labor en comercio electrónico de la OCDE. Grupos de países no-miembros - tanto mercados emergentes y economías desarrolladas - participan en las conferencias y seminarios de la OCDE y se están organizando un

[116] La Recomendación sobre la utilización de criptografía (Guidelines for Cryptography Policy) fue aprobada el 27 de marzo de 1997. Esta recomendación no tiene fuerza vinculante y señala una serie de reglas que los gobiernos debieran tener en cuenta al adoptar legislación sobre firma digital y terceros de confianza, con el fin de impedir la adopción de diferentes reglas nacionales que podrían dificultar el comercio electrónico y la sociedad de la información en general

número significativo de proyectos y eventos con especial énfasis en aspectos de política que ellos enfrentan.[117]

#### 5.6.3.1 POLÍTICA CRIPTOGRÁFICA DE LA OCDE

Recientemente, los países Miembros de la OCDE se han encargado de desarrollar e implementar políticas y regulaciones relacionadas con criptografía que en muchos países se encuentran todavía en proceso de ser desarrolladas. Diferencias en políticas pueden crear obstáculos al desarrollo de cadenas nacionales y globales de comunicación e información e impedir el desarrollo del comercio internacional. Los gobiernos de los países Miembros han reconocido la necesidad de crear una propuesta coordinada internacionalmente para facilitar el continuo desarrollo de una infraestructura de información eficiente y segura. La OCDE esta jugando un papel importante al respecto, mediante el desarrollo de consensos sobre políticas específicas, aspectos reguladores, relacionados con la cadenas de comunicación e información y tecnologías, incluyendo aspectos de criptografía.

La OCDE, ha estado activa desde hace algún tiempo en las áreas de privacidad y protección de datos y la seguridad de sistemas de información. A principios de 1996, la OCDE inició un proyecto sobre política de criptografía mediante la formación de un Grupo Ad hoc de Expertos sobre Lineamientos de Política Criptográfica bajo los auspicios del Comité de Información, Computo y Políticas de Comunicación (ICPC). El Grupo Ad hoc bajo la presidencia del Sr. Norman Reaburn de la Attomey- General Department de Australia fue el encargado de redactar los Lineamientos de Política Criptográfica (Lineamientos) para identificar los aspectos que deberán tomarse en cuenta en la formulación de políticas de criptografía a nivel nacional e internacional. El grupo Ad hoc tuvo el mandato de un año para cumplir con esta tarea y finalizó su trabajo en diciembre de 1996.

[117] Ver página Web de la OCDE, sección Comercio Electrónico, disponible en la siguiente dirección: http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-about-29-nodirectorate-no-no-no-29.FF.html

Subsecuentemente, los Lineamientos fueron adoptados el 27 de marzo de 1997 como una Recomendación del Consejo de la OCDE.

Los Lineamientos son de amplia índole y reflejan diversos puntos de vista de países Miembros. Actualmente, el Secretariado de la OCDE, tiene un Reporte sobre los Antecedentes y los Aspectos de Política Criptográfica, que explican a mayor detalle el contexto de los Lineamientos y los aspectos básicos comprendidos en el debate de la política criptográfica. Este Reporte explica la necesidad de contar con actividades internacionales y resume el trabajo relacionado llevado hasta ahora por la OCDE y otras organizaciones. El Reporte es un documento informativo que tiene el propósito de auxiliar el debate público sobre los Lineamientos, en lugar de influir en la interpretación de los mismos. En tanto que proporciona mayor detalle en el alcance de los aspectos incluidos en los Lineamientos, el Reporte no varía el significado de los Lineamientos y no debe ser utilizado como una guía interpretativa. El Reporte ha sido redactado por el Secretariado, el cual se ha beneficiado de los debates con un gran número de expertos nacionales.[118]

### 5.6.3.2 LINEAMIENTOS PARA POLÍTICA CRIPTOGRÁFICA

Los Lineamientos tienen los siguientes propósitos:

- Promover el uso de la criptografía;

- Fomentar la seguridad en infraestructuras de comunicación e información, redes y sistemas y la forma en que se utilizan;

- Ayudar a proteger la seguridad de datos y proteger la privacidad en infraestructuras de comunicación e información nacional y global, redes y sistemas;

[118] Ver página Web de la OCDE, "Sobre Política Criptográfica", disponible en la siguiente dirección: http://www.oecd.orq/oecd/paqes/home/displavqeneral/0,3380,EN-document-43-1-no-21-2864-43,FF.html

- Promover el uso de esta criptografía sin poner en riesgo la seguridad pública, ejecución de la ley y la seguridad nacional;

- Promover el conocimiento sobre la necesidad de políticas criptográficas compatibles y leyes, así como la necesidad de métodos criptográficos ínter operable, portátil y móvil en redes de información y comunicación nacionales y globales.

- Respetar los derechos de individuos, tales como privacidad, incluyendo comunicación de secretos y protección de datos personales en políticas criptográficas y en la implementación y uso de métodos criptográficos.

- Establecer los límites de responsabilidad, tanto de individuos como de entidades que ofrecen servicios criptográficos o que mantienen o que permiten acceso a llaves criptográficas.

- Apoyar a tomadores de decisiones dentro de los sectores público y privado en desarrollar e implementar políticas coherentes nacionales e internacionales, métodos, medidas, prácticas y procedimientos para el uso efectivo de criptografía.

- Facilitar el comercio internacional mediante la promoción de sistemas criptográficos móviles y portátiles a un costo efectivo;

- Promover la cooperación internacional entre gobiernos, empresas y comunidades de investigación y modelos estándar en el logro de la utilización de métodos criptográficos coordinados.

#### 5.6.3.3 ALCANCE

Los Lineamientos están principalmente dirigidos a gobiernos, en términos de las políticas de recomendación pero con la anticipación de que serán ampliamente leídos y seguidos por los sectores público y privado.

Se reconoce que los gobiernos tienen distintas y separadas responsabilidades para la protección de información que requiere seguridad en el interés nacional; los Lineamientos no están dirigidos para su aplicación en este ámbito.[119]

#### 5.6.3.4 PRINCIPIOS

Los lineamientos contienen ocho principios:

CONFIANZA EN MÉTODOS CRIPTOGRÁFICOS

ELECCIÓN DE MÉTODOS CRIPTOGRÁFICOS

DESARROLLO EN EL MANEJO DEL MERCADO DE MÉTODOS CRIPTOGRÁFICOS

1. ESTÁNDARES DE MÉTODOS CRIPTOGRÁFICOS
2. PROTECCIÓN DE PRIVACIDAD Y DATOS PERSONALES
3. ACCESO LEGÍTIMO
4. RESPONSABILIDAD
5. COOPERACIÓN INTERNACIONAL

De conformidad con la sección IV de los Lineamientos, cada uno de estos principios son interdependientes y deberán implementarse en su totalidad para balancear los distintos intereses en riesgo. Ningún principio deberá implementarse aisladamente de los demás.

[119] Los Lineamientos para Política Criptográfica se encuentran disponibles en la página Web de la OCDE en la siguiente dirección: http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-notheme- 1-no-no-10239-0, FF.html

### 5.6.4 CÁMARA DE COMERCIO INTERNACIONAL (CCI)

La CCI publicó en octubre del 2001 la segunda versión de pautas de "Uso General en el Comercio Digital Internacional Asegurado" (GUIDEC II), con el objeto de asegurar la confiabilidad de las transacciones digitales por Internet (en forma similar a las Costumbres y Prácticas Uniformes para Créditos Documéntanos, Incoterms).

GUIDEC fue originalmente elaborado por el Grupo de Trabajo de Seguridad en la Información de la CCI, bajo los auspicios del Proyecto de Comercio Electrónico de la CCI.

GUIDEC fue inicialmente elaborado y revisado en Noviembre de 1997 bajo el nombre de Prácticas Internacionales Uniformes de Autenticación y Certificación (UIACP). Durante el periodo de consultas, el título fue cambiado por el actual GUIDEC para reflejar el uso de la palabra "asegurar" en el título.

GUIDEC tiene como objetivo conjuntar elementos clave utilizados en comercio electrónico para servir como un indicador de los términos y una exposición del antecedente general al problema. También contempla uno de los problemas clave respecto a mensajes firmados electrónicamente, en que no sean firmados físicamente pero que requieren de la intervención de un medio electrónico. Esto en cambio, altera la función del firmante e introduce problemas a los que una firma física no se enfrenta, especialmente la posibilidad del uso del medio por una tercera persona. Por lo tanto, el GUIDEC adopta un término específico "asegurar" para describir lo que en otros lugares se conoce como una "firma digital" o "autenticación" en un intento por revocar el elemento de ambigüedad inherente a otros términos utilizados.[120]

[120] GUIDECII se encuentra disponible en la página Web de la CU en la siguiente dirección: htto://www.iccwbo.ora/home/auidec/auidec two/foreword.aso

### 5.6.5 ORGANIZACIÓN DE NORMAS INTERNACIONALES (ISO/IEC)[121]

La ISO ha desarrollado normas para firmas electrónicas, criptografía, autenticación y certificación, y ha participado en el desarrollo de criterios para la aceptación mutua de las autoridades de certificación, terceros confiables (sus siglas en inglés son TTP) y para la infraestructura de su gestión y uso a nivel internacional.

### 5.6.6 CENTRO DE LAS NACIONES UNIDAS PARA LA FACILITACIÓN DEL COMERCIO Y NEGOCIOS ELECTRÓNICOS (NU-CEFACT)

Provee la única norma internacional para el intercambio electrónico de datos, el "Intercambio Electrónico de Datos de las NU para la Administración del Comercio y del Transporte (NU/EDIFACT)".

### 5.6.7 UNIÓN UNIVERSAL DE SERVICIOS POSTALES (UPU)

Ha desarrollado un marco global para la seguridad de datos (servicios de encriptación) y completado una política teórica de encriptación que todas las oficinas de correos utilizarán como plantilla. También ha llegado a un acuerdo sobre las especificaciones mínimas de compatibilidad global de servicios de encriptación. La UPU también ha participado en el desarrollo de un marco global para la compatibilidad de firmas digitales, al igual que para la autenticación cara a cara, a través de establecimientos de correos a nivel mundial.

### 5.6.8 ORGANIZACIÓN MUNDIAL DE ADUANAS (OMA)

Se ha enfocado principalmente en la implantación de las normas EDI, particularmente aquellas relacionadas con el desarrollo de mensajes NU/EDIFACT de Aduanas. También está examinando temas de seguridad, tales como la autenticación y la encriptación relacionada con la transmisión electrónica de información.

[121] En la Organización Internacional de Normas ISO. La norma ISO/IEC 7498-2 (Arquitectura de Seguridad de OSI) sobre la que descansan todos los desarrollos normativos posteriores, regula los servicios de seguridad sobre confidencialidad, integridad, autenticidad, control de accesos y no repudio.

### 5.6.9 COOPERACIÓN ECONÓMICA ASIA -PACÍFICO (APEC)[122]

En la tercera reunión ministerial de la industria de información y telecomunicaciones (TELMIN) celebrada en junio de 1998 en Singapur se publicó:

"En particular, los ministros reconocieron al comercio electrónico como uno de los más importantes desarrollos de la década como promotor de los servicios de información y telecomunicaciones."

En la cuarta reunión ministerial de la industria de información y telecomunicaciones (TELMIN) en mayo del 2000 en Cancún, México se hicieron estas declaraciones:

"Se reafirma nuestro compromiso para fortalecer la infraestructura de información Asia-Pacífico para tener la capacidad de responder efectivamente al acelerado paso de la convergencia y cambios tecnológicos que traen nuevas oportunidades para la educación, salud, finanzas, investigación, comercio, desarrollo económico y social y entretenimiento.

“Se reconoce que la convergencia de servicios puede hacer surgir nuevos y complejos temas que requerirán de acercamientos innovadores para responder efectivamente y facilitar los negocios y propiciar grandes desarrollos en infraestructura y acceso a los servicios de información y de telecomunicaciones.”

En el programa de acción del Grupo de Trabajo de Telecomunicaciones {TEL) de APEC se reconocen barreras para la adopción del comercio electrónico por las

[122] APEC (Cooperación Económica del Asia-Pacífico) es un foro multilateral creado en 1989, que trata temas relacionados con el intercambio comercial, coordinación económica y cooperación entre sus integrantes. Como mecanismo de cooperación y concertación económica está orientado a la promoción y facilitación del comercio, las inversiones, la cooperación económica y técnica y al desarrollo económico regional de los países y territorios de la cuenca del Océano Pacífico.
La APEC no tiene un tratado formal, sus decisiones se toman por consenso y funciona con base en declaraciones no vinculantes.

pequeñas y medianas empresas (PYMES), donde los ministros de distintos países urgen al Grupo de Trabajo para que se aseguren ambientes políticos y reguladores que promuevan el comercio electrónico, se facilite la oferta electrónica de servicios y se mejore la infraestructura del mismo.

Respecto a la autentificación electrónica, reconocen la necesidad de promover plataformas técnicas abiertas para el comercio electrónico, donde el Grupo de Trabajo de Autentificación Electrónica propone una serie de principios.

Los retos reguladores y políticos urgen a adoptar un acercamiento de cooperación para discutir temas como convergencia, liberación de mercados y la implantación del Tratado de Libre Comercio."

**5.6.9.1 CONSIDERACIONES EN LA PREPARACIÓN DE POLÍTICAS PARA LA AUTENTIFICACIÓN ELECTRÓNICA DE APEC.**

1. El desarrollo de las tecnologías de autentificación y sus estándares asociados es primordialmente papel de la industria.

2. Existe una gran variedad de modelos de negocios, tecnologías de autentificación e implantación del comercio electrónico. Debe permitirse una libre selección de ellos y sus implementaciones.

3. Debe reconocerse que en las autentificaciones y transacciones electrónicas, múltiples tecnologías pueden ser utilizadas.

4. Cuando se desarrollen marcos legales y reguladores, se debe considerar el rol de tecnologías múltiples.

5. Marcos legales y reguladores que se enfoquen en tecnologías específicas pueden impedir el uso de tecnologías múltiples.

6. La cooperación entre economías facilita el reconocimiento transfronterizo de la autentificación electrónica.

7. Proyectos piloto de comercio electrónico entre economías permitirá el entendimiento de los temas involucrados.

8. El análisis del trabajo en otras economías y de organismos internacionales y el intercambio de información pueden facilitar el reconocimiento transfronterizo de la autentificación electrónica. APEC esta involucrada en un programa de talleres para facilitar el intercambio de información.

### 5.6.9.2 ANTEPROYECTO DE ACCIÓN DE APEC SOBRE COMERCIO ELECTRÓNICO

Los Ministros de APEC, reconociendo el enorme potencial del comercio electrónico para expandir las oportunidades de negocios, reducir costos, incrementar la eficiencia, mejorar la calidad de vida y facilitar la gran participación de pequeñas empresas en el comercio global, así como tomando en cuenta los diferentes estados de desarrollo de las economías miembros, los diversos marcos reguladores, sociales, económicos y culturales; y tomando en cuenta que mejorar la capacidad del comercio electrónico entre las economías de APEC, es necesaria para alcanzar sus beneficios, se acordó lo siguiente:

1. El sector de negocios juega un papel de liderazgo en el desarrollo de las tecnologías, aplicaciones, prácticas y servicios del comercio electrónico.

2. El papel de los gobiernos es promover y facilitar el desarrollo y despegue del comercio electrónico mediante lo siguiente:

Proporcionar un ambiente favorable, incluyendo los aspectos legales y reguladores que sean predecibles, transparentes y consistentes;

Propiciar un ambiente que promueva la confianza entre los participantes del comercio electrónico;

Promover el funcionamiento eficiente del comercio electrónico intemacionalmente permitiendo, en la medida de lo posible, el desarrollo de marcos domésticos que sean compatibles con las normas y prácticas internacionales cambiantes.

Volverse un usuario líder para catalizar y encauzar el mayor uso de los medios electrónicos.

**3.** Para que el comercio electrónico florezca, el sector privado y el gobierno deben cooperar en la medida de lo posible para asegurar el desarrollo de una alcanzable, accesible e ínter operable infraestructura de información y comunicaciones.

**4.** Cuando se reconozca que algún grado de regulación sea necesaria, soluciones tecnológicamente neutrales, basadas en la libre competencia, que puedan ser protegidas por políticas de competencia y auto-regulación de la industria, deben ser favorecidas.

**5.** El gobierno y la industria deben cooperar para desarrollar e implantar tecnologías y políticas que brinden confianza, comunicaciones confiables y

seguras, sistemas de entrega y de información que contengan temas como privacidad, autentificación y protección al consumidor.[123]

### 5.6.10 ÁREA DE LIBRE COMERCIO DE LAS AMERICAS (ALCA)[124]

Los Miembros del ALCA, tomando en cuenta la rápida expansión en el uso de Internet y del comercio electrónico en el Hemisferio y con el propósito de aumentar y ampliar los beneficios que se derivan del mercado electrónico, aceptaron una oferta de CARICOM para dirigir un Comité conjunto de expertos del sector público y privado encargado de hacer recomendaciones en las siguientes reuniones Ministeriales.

#### 5.6.10.1 EL COMITÉ CONJUNTO DE EXPERTOS DEL GOBIERNO Y DEL SECTOR PRIVADO SOBRE COMERCIO ELECTRÓNICO DEL ALCA.

El Comité Conjunto de Expertos del Gobierno y del Sector Privado sobre Comercio Electrónico del ALCA (Comité Conjunto) fue instituido por los Ministros de Comercio del Hemisferio Occidental mediante la Declaración Ministerial de San José de Marzo de 1998, respaldada posteriormente por los Jefes de Estado en la Declaración de la Cumbre de Santiago, de Abril de 1998.

El Comité Conjunto ha celebrado once reuniones desde el mes de octubre de 1998. La última reunión se celebró en la Ciudad de Panamá, los días 24 a 26 de octubre de 2001. En estas reuniones asisten delegados de los siguientes 19 países: Argentina, Barbados, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Estados Unidos, Honduras, México, Panamá, Perú, República Dominicana, Trinidad y Tobago, Uruguay y Venezuela. Dentro de los temas que se han desarrollado a lo largo de esta reuniones, se encuentran

[123] Mayor información sobre APEC BLUEPRINT FOR ACTION ON ELECTRONIC COMMERCE se encuentra disponible en el siguiente sitio: http://www.apecsec.orp.sp/

[124] El Área de Libre Comercio de las Américas o ALCA es un proyecto de integración comercial en el continente americano. La iniciativa nació en la primera Cumbre de las Américas celebrada en la ciudad de Miami, Estados Unidos, en diciembre de 1994 y en su versión original contemplaba la gradual reducción de las barreras arancelarias y la inversión en 34 países de la región (todos menos Cuba) y los paises independientes.

privacidad; protección al consumidor; seguridad; autenticación y certificación de firmas digitales; responsabilidad penal y civil; impuestos y sistemas de pagos; acceso e infraestructura; pequeñas y medianas empresas y otros temas de carácter informativo, tales como propiedad intelectual, tributación y distribución de contenidos en línea. El trabajo futuro de el Comité Conjunto se concentrará en temas relacionados con protección al consumidor, gobierno electrónico entre otros.[125]

### 5.6.10.2 INFORMES CON RECOMENDACIÓN A LOS MINISTROS DEL ALCA.

El Comité Conjunto, tiene instrucciones del Comité de Negociaciones Comerciales, de redactar informes y dirigir recomendaciones a los Ministros del ALCA con el objeto de incrementar y ampliar los beneficios del comercio electrónico y, en particular, de la manera de abordar el comercio electrónico en las negociaciones del ALCA.

En el segundo informe del Comité Conjunto, del 22 de Noviembre del 2000 se trataron entre otros temas, el de Certificación y Autenticación y basados en las recomendaciones hechas en el primer informe, el Comité Conjunto hizo las siguientes recomendaciones a los Ministros en relación al tema.

**1.** Adoptar medidas para identificar y eliminar barreras legales que impidan el reconocimiento de transacciones electrónicas, incluido el reconocimiento de la validez legal de la escritura, firma y otras tecnologías de autenticación y certificación otorgadas por procedimientos electrónicos, tomando en consideración las estipulaciones habilitantes del Modelo de Ley sobre Comercio Electrónico (Model Law on Electronic Commerce) CNUDMI de 1996;

[125] Mayor información sobre El Comité Conjunto de Expertos del Gobierno y del Sector Privado sobre Comercio Electrónico del ALCA se encuentra disponible en el siguiente sitio: htto://www.ftaa-alca.org/socomm/Commec s.aso

**2.** Esforzarse para que la legislación sobre firmas electrónicas sea neutral en cuanto a la tecnología aplicada;

**3.** Asegurar la validez legal de los registros y evidencia electrónica para su uso en tribunales y otros procedimientos oficiales, independientemente de la tecnología de autenticación o certificación utilizada;

**4.** Reconocer a las partes de una transacción la libertad de determinar por medio de un acuerdo de derecho privado, los métodos tecnológicos y comerciales de autenticación apropiados y otorgar efecto legal al acuerdo de las partes, incluyendo otros medios de solución de diferencias, sin perjuicio de las normas de orden público aplicables;

**5.** Reconocer la importancia del papel que toca desempeñar al sector privado en el desarrollo e implementación de tecnologías de autenticación y certificación y promover la participación de todos los sectores sociales involucrados en el proceso de formulación de políticas y regímenes legales en esta materia;

**6.** Procurar que las leyes o normas, no discriminen los métodos o proveedores de servicios de autenticación electrónica, nacionales o extranjeros, y que no creen barreras al suministro de servicios de autenticación por cualquiera de ellas; y

**7.** Trabajar con el sector privado para alentar la creación y utilización de sistemas de autenticación que ofrezcan una adecuada protección contra el fraude y el robo de identidad, que sean consistentes con el respeto a la privacidad de los individuos y que no creen barreras para su uso.**"**[126]

[126] 43 El Segundo Informe de El Comité Conjunto con Recomendaciones a los Ministros de fecha 22 de Noviembre del 2000, se encuentra disponible dentro de la página web del ALCA en la siguiente dirección: htto://www.ftaa-alca.org/socomm/Commec s.aso

### 5.6.11 BARRA AMERICANA DE ABOGADOS (ABA) (AMERICAN BAR ASSOCIATION)

El Comité de Seguridad de Información (El Comité) de la División de Comercio Electrónico (La División) de la Asociación de la Barra Americana (ABA), ha sido el punto focal de diversas iniciativas de ley sobre comercio electrónico seguro, desde la creación de la División en 1992. El Comité investiga información actual sobre aspectos de seguridad, incluyendo aquellos relacionados con infraestructura de llave pública, criptografía, análisis de riesgo, estándares, "racionalidad comercial" y la eficacia jurídica del comercio digital seguro.

El Comité ha expedido los Lineamientos para la Evaluación de Infraestructura de Llave Pública (PKI Assesment Guideliness), en los sucesivo PAG.

PAG ofrece una guía práctica para la evaluación y contribución, determinando el cumplimiento de políticas establecidas y licencia del PKI. Será también especialmente útil para auditar a la comunidad. Este documento esta dirigido a dos tipos de usuarios:

En primera, servirá de guía para aquellos proveedores que utilicen PKI. PAG comprende los elementos técnicos y de negocios que un proveedor de PKI deberá revisar y la importancia de establecer los elementos observados.

El segundo tipo natural y corolario de usuario son aquellos que proporcionen productos y servicios sobre PKI. PAG comprenderá principios generales de los elementos de operaciones y procedimientos que se revisarán por los proveedores de PKI, ambos técnicos y comerciales mediante los asesores de las prácticas de PKI.[127]

[127] La página del Comité de Seguridad de Información de la División de Comercio Electrónico de la Asociación de la Barra Americana (ABA) se encuentra en la siguiente dirección: http://www. abanet. org/scitech/ec/isc/

### 5.6.11.1 LINEAMIENTOS DE FIRMAS DIGITALES {DIGITAL SIGNATURE GUIDELINES)

Los Lineamientos de firmas digitales fueron el resultado de cerca de cuatro años de reuniones con la participación de expertos técnicos, legales y de negocios de más de ocho países.

El Comité de Seguridad de Información de la Sección de Ciencia y Tecnología de la ABA ha publicado los Lineamientos de Firmas Digitales (Lineamientos), que son un declaración abstracta de principios cuyo propósito es servir como una fundación de unificación de largo plazo para la ley de firma digital a través de diversos marcos jurídicos, ya sea para uso adjudicatario o para aprobación legislativa. Los lineamientos incluyen definiciones, principios generales y definen los derechos y obligaciones de las autoridades de certificación, suscriptores, (es decir, aquellas personas a quienes se les han extendido certificados) y partes que confían (es decir, personas que utilicen estos certificados para autenticar mensajes). También, articulan expectativas jurídicas en cuanto al resguardo de firmas digitales en general.

Los lineamientos son significativos, en cuanto a que son la primera (y preeminente) declaración de principios legales para certificados basados en el uso de firmas digitales. Resultan particularmente importantes en la ausencia de una ley específica sobre la materia.

Los Lineamientos fueron inicialmente incluidos en la página Web de la ABA durante el periodo de comentarios (que terminó el 15 de Enero de 1996), tiempo durante el cual aproximadamente 3, 400 copias fueron descargadas.

Los Lineamientos de Firma Digital fueron publicados y dados a conocer en la Conferencia Anual de la ABA en Agosto de 1996. [128]

### 5.6.12 GLOBAL BUSINESS DIALOG ON ELECTRONIC COMMERCE (GBDE)

En la conferencia inaugural del GBDe (1999), ante representantes de Gobiernos, Empresas Privadas y Organizaciones Internacionales de todo el mundo, se propuso el establecimiento de un dialogo al mas alto nivel, emitió una serie de recomendaciones internacionales y estableció una serie de grupos de trabajo para generar y presentar iniciativas de regulación internacional:

1. **Autenticación y Seguridad** (NEC) cada gobierno debe establecer el mínimo marco legal para asegurar la efectividad de los métodos de autenticación electrónica, previniendo fraudes.

2. **Garantía de Confidencialidad** (DAIMLER CHRYSLER) Las empresas y el Gobierno tienen la responsabilidad de garantizarla, proveyendo de reglas claras y transparentes. Asimismo para el caso de conflictos establecer reglas claras para la elección de la ley aplicable así como competencia del tribunal, y el establecimiento de un medio simple, barato y conveniente para los consumidores, para resolver en forma alternativa problemas que se pudieren presentar.

3. **Contenidos** (WALT DISNEY) El gobierno debe reconocer la libertad de expresión en Internet de la misma manera en que la reconoce para cualquier otra forma de comunicación.

[128] Los lineamientos se encuentran disponibles en la sección de publicaciones de la ABA en la siguiente dirección: http://www. abanet.org/scitech/ec/isc/dsgfree. html

4. **Infraestructura de la Información y Acceso de Mercados** (NORTEL) Independientemente del tipo de empresa que provee el servicio, los gobiernos deben de garantizar equidad en el trato a los distintos proveedores sean nacionales o extranjeros y eliminar restricciones a la inversión extranjera.

5. **Derechos de Propiedad Intelectual** (FUJITSU) Refuerzo y ratificación a lo establecido en los tratados internacionales sobre el copyright (WIPO).

6. **Jurisdicción** (EDS) Tanto los gobiernos, como las agrupaciones internacionales, deberán promover la adopción de políticas que promuevan la libertad de contratación entre proveedores y consumidores. En ausencia de definición contractual de la ley aplicable se procurará que sea la legislación y tribunales del domicilio del proveedor.

7. **Responsabilidades** (TELEFÓNICA) Se procurará establecer un marco legal basado en el principio "el culpable debe de pagar de inmediato".

8. **Protección de datos personales** (TOSHIBA) Cualquier restricción al flujo de información puede tener efectos negativos. Se deberán establecer mecanismos auto regulatorios de la misma manera y condiciones en que se protege en cualquier otra forma de comunicación.

9. **Impuestos y Tarifas** (DEUTSCHE BANK): Se recomienda a los gobiernos de hacer permanente el acuerdo temporal que suscribieron ante OMC de no imponer impuestos o derechos a las transmisiones por Internet.

Es necesario asegurar que los gobiernos no adopten una política reguladora tan severa que inhiba el desarrollo del comercio electrónico, sino que intervengan

proporcionando un transparente y armónico medio legal en el cual los negocios y el comercio puedan desarrollarse.[129]

Por otra parte, este papel sugiere una serie de principios, la articulación de políticas y el establecimiento de bases para las discusiones internacionales y tratados para facilitar el crecimiento del comercio en Internet, estos principios son:

#### 5.6.12.1 EL SECTOR PRIVADO DEBE SER LÍDER.

Si bien el gobierno ha jugado un papel importante en el desarrollo inicial de Internet, la expansión de la RED ha sido conducida primariamente por el sector privado. Para que florezca el comercio electrónico, el sector privado debe continuar a la cabeza.

#### 5.6.12.2 LOS GOBIERNOS DEBEN EVITAR RESTRICCIONES AMPLIAS AL COMERCIO ELECTRÓNICO.

Cuando dos partes desean entablar un acuerdo para la compra y venta de productos y servicios a través de Internet, deben ser capaces de realizarlo con la mínima intervención gubernamental. Los gobiernos deben frenar la imposición de nuevas e innecesarias regulaciones, procedimientos burocráticos o nuevos impuestos o tarifas a las actividades comerciales que tienen lugar vía Internet ya que, limitando en esta forma las actividades comerciales limitarán innecesariamente la disponibilidad de los productos y servicios y provocará un considerable aumento en los precios de los mismos y distorsionarán el desarrollo del mercado electrónico.

[129] Este punto es muy importante y en él insistiremos en reiteradas ocasiones a lo largo del presente trabajo, puesto que es necesario para lograr una adecuada legislación de los medios electrónicos.

**5.6.12.3 DONDE LA INTERVENCIÓN GUBERNAMENTAL ES REQUERIDA DEBE SER PARA APOYAR Y REFORZAR UN PREDECIBLE, CONSISTENTE Y SIMPLE AMBIENTE LEGAL PARA EL COMERCIO.**

En algunas áreas, los tratados entre gobiernos serán necesarios para facilitar el comercio electrónico. En estos casos, el gobierno debe establecer un estable y simple ambiente legal basado en descentralización y un esquema contractualista de la ley. Este armónico marco legal debe enfocarse en la protección a los consumidores de vendedores fraudulentos, proteger la propiedad intelectual de la piratería, proteger la privacidad, asegurar la competitividad, eliminar la intromisión y crear procedimientos simples para la resolución de controversias.

**5.6.12.4 LOS GOBIERNOS DEBEN RECONOCER LAS CUALIDADES ÚNICAS DE INTERNET**.

Todos los gobiernos deben reconocer que el genial y explosivo éxito de Internet debe ser atribuido en parte, a su naturaleza descentralizada. Los gobiernos deben también reconocer que la estructura única de Internet posee cambios significativos en los retos logísticos y tecnológicos respecto de los medios reguladores comunes y deben ajustar sus políticas adecuadamente.

Los gobiernos deben además, fortalecer la evolución de la regulación propia de la industria y apoyar los esfuerzos de las organizaciones del sector privado para el desarrollo de mecanismos que faciliten la exitosa operación de Internet.

**5.6.12.5 EL COMERCIO ELECTRÓNICO EN INTERNET, SERIA FACILITADO EN UNA BASE INTERNACIONAL.**

Además del reconocimiento de las diferencias en los sistemas locales y nacionales, el marco legal que apoye las transacciones en Internet, debe ser

gobernado por principios consistentes independientes de los países en los cuales el comprador o el vendedor reside.[130]

Existe, por otra parte, la creencia generalizada que debe ser el propio mercado en vez de los gobiernos, el que debe determinar los estándares tecnológicos y otros mecanismos para la interoperabilidad, la tecnología se mueve muy rápido para los gobiernos para tratar de establecer estándares tecnológicos para el gobierno de Internet y cualquier intento de hacerlo, sólo crearía el riesgo de la inhibición de la innovación tecnológica.

Los estándares son críticos para el éxito comercial de Internet a largo plazo para conjuntar productos y servicios de múltiples vendedores para que trabajen juntos o ínter operen, esto además, refuerza la competencia y Reduce la incertidumbre en el mercado global.[131]

Para asegurar el crecimiento del comercio global electrónico en Internet, los estándares

serán requeridos en diversas áreas, tales como:

**1.** Sistemas de pago electrónico.
**2.** Seguridad (confidencialidad, autenticación, integridad control del acceso, etc.)
**3.** Infraestructura de servicios de seguridad.
**4.** Sistemas de protección electrónicos del copyright.
**5.** Catálogos electrónicos.
**6.** Conferencias en video y en datos.
**7.** Tecnología de alta velocidad en los canales de los datos.[132]

[130] Guibourg, Ricardo y otros, "Manual de Informática Jurídica", Editorial Astrea, p. 57, Buenos Aires, 1996.
[131] Op. Cit. Nota 4, p. 16.
[132] A Framework for Global Electronic Commerce, Srnith & Lyons Information Technology page, 1999; www. smithlyons. ca/if/welcome.htm

Corno se ha podido apreciar, de la anterior exposición, el actual y el ulterior desarrollo de Internet, requiere una participación conjunta de todos los sectores que intervienen en su funcionamiento y desarrollo, no sólo se requiere que los gobiernos realicen esfuerzos conjuntos para la elaboración de disposiciones uniformes aplicables al comercio electrónico, sino que, además se requiere de la participación significativa del sector privado, en especial de la industria en general que viene a ser el principal interesado en el desarrollo de dicho tipo de comercio, ayudando en la elaboración de estándares y tecnologías de punta que permitan el logro de un entorno legal armónico que permita el correcto desarrollo del comercio a través de Internet.

**RECOMENDACIONES INTERNACIONALES:**

**1.** Reconocimiento jurídico internacional de los contratos y transacciones electrónicas en Internet, basado en normas uniformes a nivel local.

**2.** Estándares internacionales para la firma digital y entidades certificadoras.

**3.** Orden internacional para evitar abusos en el registro de nombres de dominio.

**4.** Confianza y protección a los Consumidores.

**5.** Políticas sobre los contenidos en Internet: Protección al patrimonio e identidad cultural; Evitar y/o sancionar contenidos ilícitos.

**6.** Políticas de libre acceso a las telecomunicaciones.

**7.** Protección de la Propiedad Intelectual.

8. Reglas nacionales e internacionales de jurisdicción y competencia para la solución de controversias.

9. Normas de responsabilidad legal y delitos informáticos.

10. Protección de los datos personales del individuo y flujo de datos transfronterizos.

11. Reglas sobre impuestos y tarifas arancelarias.

# CAPITULO VI

# CAPITULO VI

## CONCLUSIONES Y RECOMENDACIONES

En el trabajo se ha tratado de dar una idea de los cambios tan importantes que ha experimentado la firma desde sus orígenes hasta nuestros días y como debemos tratar de adaptar estos cambios a la realidad social y dejar la puerta abierta a otros futuros cambios y otras nuevas tecnologías que sin duda vendrán.

- ✓ Las nuevas tecnologías de la información y las comunicaciones, unidas a otras técnicas dan fiabilidad al documento electrónico y tratan de lograr una mayor seguridad mediante el desarrollo y extensión de remedios técnicos y procedimientos de control basados en la criptografía.

- ✓ Esta mayor seguridad que se pretende con una adecuación normativa nos conducirán hacia la autenticación electrónica. El miedo que existe a estas nuevas tecnologías de la información no está en la electrónica, ni en las comunicaciones sino a su mala utilización debido a la no formación y adecuación de las personas y medios a la realidad social.

- ✓ La creación de los fedatarios públicos electrónicos nos llevará a unas garantías superiores en la autenticación de los documentos que circulen a través de las líneas de comunicación, así como la creación de un fichero público de control con mayores garantías de las actuales.

- ✓ Una única Entidad de Certificación de ámbito universal es inviable, por tanto deberán existir una o varias redes de autoridades nacionales o sectoriales, interrelacionadas entre sí y que a su vez den servicio a los usuarios de sus ámbitos respectivos.

- ✓ La Electrónica Avanzada, con las garantías exigidas por una cada vez más necesaria seguridad jurídica, puede abrir un prometedor camino que deje en entredicho la eficacia real de la fe pública tradicional.

- ✓ El uso de Internet y el Comercio Electrónico en El Salvador han tenido un crecimiento considerable en los últimos años, lo que abre las puertas a nuevas oportunidades para el desarrollo económico del comercio tanto a nivel local como internacional y contribuye a la creación de nuevas fuentes de empleo; lo anterior obliga a replantearnos cuestiones del comercio tradicional las cuales van desde la validez legal de las transacciones, contratos sin papel hasta la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio electrónico.

- ✓ Para asegurar las transacciones del comercio electrónico se ha implementado el uso de la firma electrónica o digital la cual es un conjunto de datos electrónicos que identifican a una persona en concreto, suele unirse al documento que se envía por medio telemático, como si de la firma tradicional se tratara, de esta forma el receptor del mensaje está seguro de quien ha sido el emisor; este mecanismo de seguridad cumple con las características de integridad, autenticidad, no repudio y confidencialidad, con el fin de que exista una celebración válida de negocios jurídicos que impliquen la viabilidad de expresar la voluntad de una persona y con ello la posibilidad de celebrar contratos válidos y exigibles.

- ✓ La seguridad en las transacciones económicas es una preocupación para los responsables de los sistemas de información, es por eso que la Firma Electrónica Avanzada es el sistema más seguro para enviar datos, con la certeza de que nadie mas que el receptor autorizado será capaz de leerlo,

ya que hoy por hoy es el mejor método para garantizar la seguridad en las transmisiones de datos a través de la red porque aplica el máximo nivel en el encriptamiento de la información que protege.

- ✓ El fundamento de las firmas digitales es la criptografía, ya que es una ciencia que se ocupa de la transformación de mensajes en formas aparentemente ininteligibles para el lenguaje humano y posteriormente devolverlos a su forma original, lo cual permite proteger la integridad de los mensajes transformando los datos en signos ilegibles y solo los revela si se le aplica la clave para desencriptarlos.

- ✓ Las entidades de certificación son una pieza fundamental en el desarrollo del Comercio Electrónico, pues son los que brindan certeza sobre el autor y contenido de un mensaje de datos o permiten conocer a los emisores de una oferta y aceptación de actos jurídicos y las partes intervinientes en un contrato; por lo mismo de ellas depende el desarrollo de este tipo de canales de comunicación dentro de un marco de seguridad jurídica esencial para la proliferación del comercio por esta vía. Además permiten evitar que se cometan fraudes por falsificación de identidad o que se caigan en errores contractuales por falta de personería jurídica.

- ✓ Las transacciones del comercio electrónico revisten seguridad y certeza, sin embargo, no están libres de enfrentarse a situaciones conflictivas debido a la dificultad de acordar transacciones o por el incumplimiento de alguna cláusula contractual; ante esta circunstancia se plantean la sustitución de la actuación judicial por formulas de solución extrajudicial, tales como la mediación, conciliación o arbitraje, mas acordes con lo característico que presenta la red y los conflictos derivados de su uso.

- ✓ Los mensajes y documentos electrónicos constituyen la forma en que los comerciantes y usuarios de los medios electrónicos realizan la mayoría de las transacciones comerciales, por lo tanto tendrán eficacia probatoria, si además de ser validos reúnen los requisitos de idoneidad y son conducentes para probar un hecho, además debe tener establecida su autenticidad.

- ✓ La sociedad salvadoreña que esta por ingresar a la cultura informática necesita de un soporte jurídico que despeje las inquietudes que plantea la realización de actividades a través de Internet, así como el uso de nuevos medios para dar rapidez a las transacciones comerciales que permitirán a nuestro País aumentar su productividad, competitividad y así reducir tiempo y costo.

- ✓ El intento de regular el comercio electrónico y principalmente la Firma Electronica Avanzada queda limitado a establecer casos especiales que se adaptan a circunstancias específicas, tal es el caso de las aduanas, lo cual no es suficiente para proteger jurídicamente y poder determinar los mecanismos necesarios que permitan a lo usuarios de este sistema tener seguridad al utilizarlo.

## RECOMENDACIONES

- ✓ El Estado salvadoreño es el que debe analizar y adoptar los mecanismos y sistemas que se están generando con la finalidad de brindar protección y garantía a las personas que interactúan dentro de los modernos medios de comunicación y contribuir al fortalecimiento de la educación, investigación y

ampliación de los conocimientos tecnológicos relativos al uso de los medios informáticos y de esta manera hacerlo accesible a la población en general.

- ✓ Es necesario hacer un análisis exhaustivo, sistemático, serio y coherente de la actual legislación tanto sustantiva como procesal con la finalidad de concluir cual es el idóneo y cual debería ser derogado para establecer un nuevo cuerpo legal mas valido, sólido y que brinde una mejor protección jurídica a las relaciones que se dan por medios electrónicos y a la vez establecer mecanismos procesales que permitan exigir el cumplimiento de obligaciones que se pactan por dichos medios.

- ✓ Es preciso la creación de entidades certificadoras abiertas que faciliten la aplicación del comercio electrónico en todos sus ámbitos, ya que al existir en nuestro medio una entidad certificadora cerrada limita el tipo de transacción a realizar y por ende el desarrollo del comercio electrónico en El Salvador.

# BIBLIOGRAFÍA


- BARCELÓ, ROSA JULIA Y VINJE, THOMAS. “Hacia un marco Europeo sobre Firmas Digitales y Criptografía” Revista de Derecho Mercantil N° 228, abril-junio 1998.

- CABANELLAS DE TORRES, GUILLERMO, Diccionario Jurídico Elemental, Editorial Heliasta S. R. L. Buenos Aires, 1994.

- CUBILLOS VELANDIA, RAMIRO Y OTRO, Introducción jurídica al comercio electrónico, Ediciones Jurídicas Gustavo Ibáñez, Bogotá (Colombia), 2002.

- MARTÍNEZ NADAL, APOL-LONIA, La Ley de Firma Electrónica, Segunda Edición, Editorial Civitas, Madrid (España), 2001.

- PALLARES EDUARDO, Diccionario de Derecho Procesal Civil, Séptima Edición, Editorial Porrua, S.A. México, 1973. Pág.

- RIVAS HERNÁNDEZ, SALVADOR ANTONIO Y OTRO, La Firma Electrónica. Monografía. Universidad Francisco Gavídia, 2004

- SARRA, ANDREA, Comercio Electrónico y Derecho, Editorial Astrea, Primera reimpresión, Ciudad de Buenos Aires, Argentina, 2001.

- GODWIN, M., “La Ley de la Red: Problemas y Perspectivas”, Internet World, 1993, p. 47.

- R. RESNICK Y D. TAYLOR, “La Guía del Negocio de Internet: Montar la autopista de información para beneficiarse”, Editorial Sams, 1994, p. XXV.

- CARROLL, J. Y BROADHEAD, R., "Manual Canadiense del Internet ", Editorial Prentice Hall, 1995, p 46.

- CAMERON, DEB. “El Internet una Oportunidad de Negocio Global”, Computer Research Corp. Journal, EUA, 1995, p. 136.

- BOLIO A. ERNESTO y LLAGUNO. JORGE A. Revista Istmo número 250 Septiembre -Octubre del 2000, artículo Creatividad e Innovación en Internet.

- Tasa constante de crecimiento, aplicada durante un periodo.

- KAHIN, BRIAN, KELLER, JAMES “Acceso Publico al Internet”, Instituto de Tecnología Press, p. 136, 1996.

- FERNÁNDEZ FLORES, RAFAEL, "La WWW una telaraña que se teje a plena luz del día", en la revista RED, no. 70, año VI, pp. 38-40, julio de 1996,

- EMERY, VINCE, “Como crecer su negocio en la red”, p. 82, Edit. Coriolis Group/IDG,1996.

- “FIRMA" Enciclopedia Jurídica Omeba, Tomo XII, Editorial Bibliográfica Argentina, pp. 290-293

- FLORIS MARGADANT G. "Derecho Privado Romano" 4a ed. Editorial Porrúa. pp. 116-119

- TOMAS Y VALIENTE FRANCISCO "El orden Jurídico Medieval" Madrid, Marcial Pons, Ediciones Jurídicas y Sociales, S.A. pp. 53-54

- ACOSTA ROMERO, Miguel; "Nuevo Derecho Mercantil"; capítulo XVIII: La firma en el derecho mercantil mexicano; página 537 a 562; Editorial Porrúa; Primera Edición; 15 de agosto del 2000.

- BRADLEY SMITH Y WAN-GO WEN, China Historia en Arte. Editorial Windfall & Co., 1972, U.S.A., Pág. 110-101, 138-139.

- CABANELLAS DE TORRES, GUILLERMO. Diccionario Jurídico Elemental, Editorial Heliasta S.R.L, Buenos Aires, Argentina, 1994. Pág. 115

- MUSTAPICH, J. M., Tratado de Derecho Notarial, tomo I.

- PLANIOL Y RIPERT, Traite Pratique de Droit Civil Frangais, tomo VI, núm. 1458.

- PLANIOL, M., Traite Elémentaire de Droit Civil, tomo II, núm. 62. Nueva Enciclopedia Sopeña. Diccionario ilustrado de la Lengua Española. Tomo II, p.1044. Editorial Ramón Sopeña, S. A. Provenza 95, Barcelona, 1955.

- STROKE PAUL, "La Firma Electrónica" Editorial Cono Sur, España, pp. 17-18.

- RUBIO VELÁSQUEZ, RODRÍGUEZ SAU, MUÑOZ MUÑOZ., La Firma Electrónica, Aspectos Legales y Técnicos, Edición Barcelona, 2004, Pág. 179.

- MARTÍNEZ NADAL, A., Comercio electrónico, Firma Digital y Autoridades de Certificación, 3ª Edición, Civitas, Madrid, 2001 Pág. 45.

- NASH, A.- DUANE,W.- JOSEPH,C-BRINK,D., PKI Infraestructura de las claves publicas, McGraw Hill, Bogota, Colombia,2002, Pág. 21y siguientes.

- PEÑALOZA EMILIO “La protección de datos personales” Editorial Díaz de Santos, España, pp. 114.

- GUERRERO, MARÍA FERNANDA. El notario virtual de los negocios en línea. Revista Ámbito Jurídico. Bogota, Colombia, Abril 2001. Pág 12

- LOPEZ OÑATE “La Certeza del Derecho Digital” Editorial Milano, España, pp. 81-84.

- GUIBOURG, RICARDO Y OTROS, "Manual de Informática Jurídica", Editorial Astrea, p. 57, Buenos Aires, 1996.


**PÁGINAS WEB**


“comercio electrónico”, www.monografia.com/trabajo12/monografias.html.

“criptografía y firma Digital”, www.webpanto.com

www.iec.csic.es/criptonomicon/seguridad

www.espanol.groups.yahoo.com/groups/

www.html.net/seguridad/varios/firma-certificado

www.html.net/seguridad/varios/firma-certificado

www.ingenieroseninformatica.org/recursos/tutoriales/firmaelectronica/cap4.php

www.internautas.org

www.scba.gov/fdweb.swf

www.cne.es/firmadigital/seguro/sisicne1/index1.asp

www.hfernandezdelpech.com.ar/leyes/trab/firma%20digital.deusto%202002.htlm

www.zonavirus.com/datos/articulos/44/firma_digital_certificados_digitales.asp

www.mailweb.udcap.mycontelect.html

www.htm/web.net/seguridad/varios/firma-jurídico.html
www.geocities.com/capitolgil/cenate8569/html.
www.virusprot.com/art.36html/trabajofirmavenezuela#.asp
http://www. nua.ie/surveys/
http://www.abcdelinternet.com/stats.htm
http://www.abcdelinternet.com/stats.htm
www.exitoexportador.com
http://www.abcdelinternet.com/stats.htm
http://www.vinculodeempresa.com.mx
www.findlaw.com
www.webopedia.com/TERM/U/URL.html
http://es.wikipedia.org/wiki/URL.
http://www.rae.es
http://www.fundacionauna.org/areas/25_publicaciones/eEspana_2006.pdf.
http://www.pcworld.com/article/id,17497-page,1/article.html.
http://www.webopedia.com/TERM/I/IP.html y http://es.wikipedia.org/wiki/Ip.
http://www.hess-cr.com/secciones/dereinfo/ dnspropiedad.shtml,
www.cis.ohio-statc-edu/hvDertext/faa/usenet/coDvríght-FAQ/Dart2/faa.html
http://www.tercerarepublica.com/articulo.php?id=25
http://www.iso.org
www.bakerinfo.com
www.vlex.com.
www.scba.gov/fdweb.swf
www.hfernandezdelpech.com.ar/leyes/trab/firma%20digital.deusto%202002.htlm
es.wikipedia.org/wiki/Bits
www.monografias.com/trabajos16/diccionario-comunicacion/diccionario-comunicacion.shtml
www.hidcorp.com/espanol/page.php

www.omega.ilce.edu.mx:3000/sites/ciencia/volumen3/ciencia3/149/htm/sec_11.htm
www.dewey.uab.es/pmarques/glosario.htm
http://snts1.jus.gov.ar/minis/Nuevo/ProyectoCodigoCivil.htm
www.nist.gov
http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343..pdf
http://www.cmt.es
http://www.bundesnetzagentur.de/media/archive/3612.pdf
http://www.bundesnetzagentur.de/media/archive/3613.pdf
http://protocollo.gov.it/normativa/dlgs10_02.asp
http://.opsi.gov.uk/SI/si2002/20020318.htm
http://www.sweden.gov.se/content/1/c6/02/72/93/569fc933.pdf
http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-about-29-nodirectorate-no-no-no-29.FF.html
http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-1-no-21-2864-43,FF.html
http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-notheme- 1-no-no-10239-0, FF.html
htto://www.iccwbo.ora/home/auidec/auidec two/foreword.aso
http://www.apecsec.orp.sp/
htto://www.ftaa-alca.org/socomm/Commec s.aso
http://www. abanet. org/scitech/ec/isc/
www. smithlyons. ca/if/welcome.htm
http://www. abanet.org/scitech/ec/isc/dsgfree. html

**LEGISLACIÓN**

- Constitución de la Republica de El Savador (D.L. 38 de 15 de diciembre de 1983, publicada D.O. de 16 de diciembre de 1983.)

- Ley de Simplificación Aduanera (D.L. 529 de 13 de enero de 1999, publicada en el D.O. de 3 de febrero de 1999.)

- Ley General Marítimo Portuaria (D.L. 994 de 19 de diciembre de 2002, publicada en el D.O. de 1 de octubre de 2002.)
- Ley de Anotación Electrónica de Valores en Cuenta (D.L. 742 de 21 de febrero 2002, publicada en el D.O. de 22 de marzo de 2002.)

- Ley de Banco (D.L. 697 del 2 de septiembre de 1999, publicada en el D.O. de 30 de septiembre de 1999.)

**TESIS**

- ALFARO NAJARRO, RENE ADONAY Y OTROS, Plan de implementación del comercio electrónico para la mediana empresa comercial Salvadoreña, Universidad Tecnológica, Facultad de Ciencias Económicas, Licenciatura en Administración de Empresas, Noviembre 2001.

- POLANCO VILLALOBOS, JOSÉ ANTONIO Y OTROS, La regulación sobre el comercio Electrónico en el ordenamiento jurídico Salvadoreño, Universidad José Simeón Cañas, Facultad de Ciencias del Hombre y la Naturaleza, Licenciatura en Ciencias Jurídicas, Noviembre 2001.

# ANEXO

- Ley Modelo de la CNUDMI sobre Comercio Electrónico con la guía para su incorporación al Derecho Interno 1996.

- Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la guía para su incorporación al Derecho Interno 2001